The Value Chain, Trust, and Lasagna

Edna Conway, chief security officer for Cisco's global value chain, on third-party partnership and trust in a hyper-connected world.

Michelle Dennedy: If you're worried about managing your third parties, you are not alone. And if you're not worried, get on that. Gartner reports that nearly 70 percent of chief audit executives reported third-party risk as one of their top concerns. But many are still struggling to manage this task. The reason? Well, it's a really hard job. Today's Sigma Rider is a shero of mine because her passion ... I can just stop that sentence there because of her passion. But it's her passion for building resiliency, continuity, security, supply, and availability into Cisco's value chain.

We'll get into the difference between a supply chain and a value chain in just a moment here, in addition to security and integrity, of course.

Cybersecurity, data protection, privacy. You like to stay ahead of the curve and listen to experts who are leading the way in deriving greater value from data with a more organized approach to data privacy. You're like us, a few deviations past the norm. You are a Privacy Sigma Rider.

Hello everyone. Michelle Dennedy here again. I'm excited to have my friend, my colleague, my fashionista icon, style guide, and colleague, Edna Conway, joining us on the podcast. Hey, Edna.

Edna Conway: Hey, Michelle. So glad to be here.

Michelle Dennedy: It's going to be a fun one. Edna is Cisco's chief security officer for our global value chain and drives a comprehensive security architecture across our third-party ecosystem, which is no small potatoes here at a multinational company.

So, Ms. Edna, without further ado, I want to talk a little bit about your credentials for a minute. And then I'm going to let you brag about yourself, and if you don't brag I may come back and do more. Is that okay with you?

Edna Conway: Oh heavens. Okey-dokey.

Michelle Dennedy: It's one of these things. If anyone was in doubt that we were the fairer sex, I think you and I are fair. But we're also, might I say because we're not FCC-regulated in that way, bad asses. If I do say so myself, and I do. Edna is recognized both here in the United States and globally with NATO as the developer of architectures that deliver value chains, security, sustainability, and resiliency. She most recently was appointed to the executive committee of the US Department of Homeland Security's ICT Supply Chain Risk Management Task Force in addition to a huge day job.

And before joining Cisco, Edna was a partner in an international private legal practice and served as an assistant attorney general for the state of New Hampshire. So, not only does she wrestle

our value chain to the ground, she can put you and would put you in handcuffs if you don't do her bidding. Welcome, welcome, Edna. We need more voices like yours.

Edna Conway: No, thank you. Rest assured, I don't carry my handcuffs anymore, so you're pretty safe.

Michelle Dennedy: That's unfortunate.

Edna Conway: Just a couple of weapons.

Michelle Dennedy: Okay, good. We won't say which ones because we're private here.

Tell me, Edna, what has been, since I met you several years ago, your most current area of focus and passion? What is a value chain versus what's a risk kind of model?

Edna Conway: I think, let's step back for a minute because I think that is an interesting differential, but here's how I like to say it. I mean, the reality is when you look at the digital world that we all participate in in an enterprise government or even individual consumer perspective, here's what's true for all of us. There are more of them who are touching virtually or physically our stuff and our information than there are of us. So, this is the day and age where, quite frankly, we both have views on this. I say in 2019, value chain security's coming to everyone's door. It's been there all along.

So, start with that premise. The value chain is this great end-to-end lifecycle of any solution, whether that solution is hardware, software, or a cloud service. And that sets the framework for who those third parties are and the wonderful productivity they can bring to us and the fantastic level of risk expansion that they also bring to our door.

Michelle Dennedy: There's a lot of concepts here that I really want to be very clear about. When you are talking about end-to-end value chain, are you talking about the data, the storyline, the systems, or who touches actual products, or delivers actual services? How do we break this down conceptually to really understand what's included in that value chain?

Edna Conway: That's a great question because we need to think about it in stages. What it means is, when I say lifecycle, think about a solution. The first way that solution comes to be is it's a fantastic idea in some creator's mind. So, the first stage is really, how do you design and develop this idea that you have for delivering something, some functionality? How are you going to then move on to, how am I going to plan on how to literally put it together, whether it's modules of code, whether it includes hardware devices, whether it's an infrastructure play? How am I going to order what I need from all those wonderful third parties who need to provide me with the pieces of what I'm going to do? How am I going to build it?

Michelle Dennedy: That doesn't just mean manufacturing, but it could. I mean—

Edna Conway: Oh heavens, no.

Michelle Dennedy: In the tangible world, it's talking to farmers who grow the corn, and then another person who maybe raises cattle, and another one who does something else. Somehow those ingredients

come together, and the outcome is a product or an offering or an experience. But what you're talking about is so much more than building actual, tangible stuff, right?

Edna Conway: That's correct. It's also how you utilize it and how we coordinate together during the course of its utilization, and how we handle it when we choose not to use it any more. How do we shut it down?

Michelle Dennedy: Yeah.

Edna Conway: What happens with the data that resided there? What happens, quite frankly, even from an environmental perspective when there's tangible equipment and how we handle that? What commitments are we going to make to one another across that lifecycle which can be as short as several days or weeks and as long as 20 to 30 years? Imagine, for example, the capacity to move data and communicate it on, if you will, the satellite systems. So, you're actually on the satellite and facilitating that. I assure you, you're not going to bring it down in six months. Not on purpose anyway.

Michelle Dennedy: Not on purpose. We hope it doesn't come down in six months. What you're really talking about is sort of bringing a system of handoffs, a system of curation, a system of delivering on objectives in a hyper-connected world. I know you've given a TED Talk on thriving in a hyper-connected world. Can you give us a few highlights of what does that concept mean in exactly as you're describing, 24/7, global, sometimes intergalactic connectivity?

Edna Conway: I think a hyper-connected world is really one that can be translated to as we connect, are we constantly aware of with whom we're connecting? It may not necessarily be the with whom you are communicating at that moment, but you are connecting with someone who made the device that you are utilizing. You are connecting with someone who is affording you functionality through that device. You are connecting with a host of people who you are communicating with independently through a device. And oh, by the way, it may simply be I'm sitting down with a group of folks who are dispersed around the globe to create the first iteration of a new solution.

We're doing that together. Do I know who I'm working with? Do I know what our goals are? What we really have to do is start to think about what we care about. It sounds like it's, oh my gosh, it's just too daunting. But at the end of the day, you really only care about certain things. You and I are aligned on a couple of things in this regard. I've always thought that ... I know you say that the actual currency of the digital world is data. I have a slightly different way to integrate with you on that. I think the currency of the digital world is trust. It's the same trust that we've had since mankind began back when we had cave people and you handed the club, the second club, to the person next to you, and you weren't quite sure whether that gentleman or woman was going to club you or the wooly mammoth you were both working on capturing. So, it's trust.

What we've done is, we've utilized data as the fuel that allows us to build that trust. And then we blend in technology, whether it's things like, I don't know, putting a dry polynomial expression on a chip inside its—

Michelle Dennedy: As you do. I mean, who doesn't derive polynomials on a chip? It's just it's practically as good as guacamole.

Edna Conway: It is better than guacamole because it lifts itself up and flags you and says, "Look here just in case you missed it." Or it could also be something as seemingly mundane but important as using a distributed ledger to add integrity to the data over the course of this lifecycle as we utilize our digital experience. That means that we're in a very new place. We're in a place where trust still is the currency. Data fuels it, but we have a reality that various technology is allowing us to build integrity into that use. And then finally I think, Michelle, we should talk a little bit about what we've been hearing for years and are just beginning to hear an inflection point and see it in reality, which is IT-OT convergence.

Michelle Dennedy: Yes. Yes. For anyone who's not into the acronymia of high tech, it's the Internet of Things and the Internet of Everything and the Internet of Experience and the Internet of Ethics. In my mind, it's all of that. When we talk about hyper-connectivity, that's the enabler. It's devices that have some sort of means of connecting to other things, other people, and other ideas, even other outcomes.

Edna Conway: I think you raised a really good point, which is there's another mantra in this hyper-connected world. We can't do it alone any longer.

Michelle Dennedy: That's right. That's right.

Edna Conway: And that's a different model. That's why you see things like the Charter of Trust in Europe started by a couple of companies and Cisco has the privilege of participating in that. It has 10 fundamental principles, but let's say the name again. It's not the Charter of Technology. It's not the Charter of Data. It's not the Charter of Chips. It's the Charter of Trust. It has 10 fundamental principles. One of the principles that I'm deeply involved in is, how do we secure the digital supply chain or value chain? What does that really look like in this world you just described of a connectivity that includes ethics, humanity, human behavior? It includes technology, both tangible and intangible, and usage. That's a new model.

Michelle Dennedy: It's a really new model. It's a new approach. I think what you're highlighting here is a big part of this value chain. Value chain security, value chain trust, value chain curation is really understanding that there's no law that's going to save you. There's no technology that's going to save you. There's no training and people skills and process that's going to save you. It's an integration and a leveraging of the best of all of those things together and then having a systematic way of making sure that you've done it when it's done.

Edna Conway: I think that's a great way to segue into something. I had the privilege of speaking at an industrial controls conference relatively recently, and that's interesting when you come from the information technology world. You're talking to people who are working in operational arenas, hardcore industrial operations. The analogy that I used to talk about things like practical segmentation, which to those of us on the IT side, network segmentation comes as segmentation 101, how to run a decent network. Forget a best-in-class network, you just need to do this for a variety of reasons: redundancy, availability, and most importantly, security.

Michelle Dennedy: Yeah. Making it work.

Edna Conway: Right. We talked about lasagna. What I said to them was—

Michelle Dennedy: As you do, Edna.

Edna Conway: Lasagna, as you know, has been a part of my life since birth, with two Italian parents. We talked about the fact that segmentation is fantastic, but you need to understand that you're only as good as the sum of your third-party ecosystem. So, quite frankly, the richness of a lasagna without the cheese might be different. And the richness of a lasagna without thinking about the fact that it takes equipment and oven to heat it would not be as effective or delicious. Or, more importantly, if you haven't thought about the human behavior of that teenager who's going to walk into your kitchen and actually come home from school and take the bloody lasagna out of the oven because they want XYZ snacks and forget to put it back in, there's a little bit of an operational process played in there too, isn't it?

Michelle Dennedy: Not that that would happen in our homes.

Edna Conway: These are the kinds of ways that we can describe things that we've all been dealing with in life and how we approach our digital environment in that degree of hyper-connectivity and piece it out. What are the steps? How are we working together? What are we doing to drive consistent and relentless security in each of those environments in a practical way, not in an expensive way, and not in a way that is daunting, but a way that fits into what you're already doing?

Michelle Dennedy: Yeah. Let's call the lasagna, data. Imagine that there were not just your teenager who's inadvertently not putting it back in the oven, but the minute you turn your back, someone else is taking your lasagna out and maybe dumping it in the yard or maybe filling it with leaves or grass and spoiling that lasagna. There's a recent headline that US firms alone are expected to spend $19.2 billion on third-party data management this year to get it going where it wants to go despite all of these massive privacy concerns and fines and fees from other legislative schemas internationally.

How do we look at that data lasagna, protect it, and think about how does the systematic approach deal with regulation and law in addition to the technology challenge?

Edna Conway: It's a great thought process. I think that the solution is an integrated architecture, an integrated architecture that hopefully makes it somewhat simplistic. You know for years I've been driving in architecture, and we incubated it here at Cisco in the supply chain operations organization, which is manufacturing. We've expanded it into the value chain, partnering with development folks on how do we get this third-party view into our secure development lifecycle? Because it's great if you're developing things securely in isolation, but what about all the third parties?

How do we then look down the road and say, "How do we integrate this in an architectural way with those who are providing the services or offerings or the services for software updates, et cetera?" And then what do we do, in all honesty, with those third parties that's unique? You can imagine you wouldn't ask, for example, somebody who is providing transportation logistic services for hardware the same kind of security questions as you would for a third-party cloud service provider who's providing you with storage or compute capacity. They're doing different things.

And yet, a meaningful architecture that identifies core domains that you're worried about can actually drive all of you together in a way that's efficient and effective based on the unique nature of what that third party does in your ecosystem.

Michelle Dennedy: Yeah. I think you're touching on why ... and I'm going to call it. We'll see if you're listening after 2019. I'm calling 2019 the year of the third party, not just because we've spent last year, 2018 was the year of GDPR and mapping our data. Now we're recognizing exactly what you're saying, that there are different needs and different management styles and requirements for different types of third parties, but at the same time, there's a common thread of data that runs through them.

For example, one of the most legendary hacks and thefts was the massive Target breach a few years back that really was facilitated by non-management of a heating and cooling vendor, someone you would never put into your data risk map necessarily. So, it's not just about risk. As you say, it's really about reliance on these third parties. I would love to get your thoughts on how do we establish and maintain this meaningful trust in this digital economy with these third parties in particular?

Edna Conway: We started this with a discussion about, it is about the human element and ethics and partnership and trust. You can have all the architecture and all of the technology in the world, what you also need is a relationship. You cited a really important statistic about the expenditure that we're going to see in the coming year. I think we should be aware of the fact that despite all of our efforts as we expand the denominator, we're not really seeing much movement on third-party risk success, and here's my data to support that.

I did an analysis of ... We're all familiar, certainly in the US and in many international locations, the Verizon data breach investigation report. I looked at it over the last eight years. Over the last eight years, Michelle, the average security incidents, and you know not all of them are attributable, but where they're attributable that are linked to third parties, has hovered between 74 and 80 percent.

Michelle Dennedy: That's right.

Edna Conway: So, averaging about 76 percent over eight years. That's really not moving the needle. And let's be honest, statistically we have to say, well, of course the number of third parties is growing, Edna. So, the denominator has grown, so you have to be fair about the math. But to me, that's a failing grade. What that means is you need to have a partnership. You need to sit down and say with your partners, "What am I worried about?" We've been very clear about that. I'm worried about taint. I'm worried about the alteration of any solution in any way other than I intended or authorized.

I'm worried about counterfeit at both the raw material and finished good level, counterfeit code modules, counterfeit service offerings, you name it. We're also worried about the information security health of our third-party ecosystem because to your point that in a hyper-connected world, you can lock down, as you know, our fabulous CSO has, your own environment. But those third parties still need to be in partnership with you at the end of the day. That HVAC vendor that you just pointed out could be servicing a third party who is servicing a third party who is still affecting a solution that you actually offer, and the next thing you know, you're infected.

Michelle Dennedy: Right. Exactly. When we tell our kids or our spouses even, "It's not your driving that I'm as worried about. It's everyone else's." So, you have to take a defensive mode on your own. And then you have to make sure that there are rules to the road, that they're clear, that people understand them, that people are following them, and they're held into account when they're not being followed.

Edna Conway: I think that's a fair assessment. I see more colleagues coming to the table. I mean we had the privilege years ago of contributing to the first ISO standard 20243 that talked about, how is a commercial off the shelf provided? Do you actually establish that you're a trusted vendor? Not that this particular solution is trusted, or not that this network meets an ISO information security standard, you holistically are trusted. That was an interesting way to start to blend what I think we're going to see in 2019 and beyond, the beautiful woven mosaic that we're putting together with the increased digitization, but more importantly, the fact that it's now in our practical daily operational lives.

Michelle Dennedy: That's fantastic.

Edna Conway: It's in our power grids. It's in our machinery and our equipment, and we could probably spend six days talking about what fun it's going to be to actually just eat your lasagna and then walk out the door and say, "I'm too bloody tired to drive, so I'm just going to ring up my automated vehicle." And autonomously it's going to say, "Yes, we know that you would like the heater on and we would also know that since you've just had your lasagna, want classical music, Edna, preferably Grieg." I would like the Peer Gynt Suites to lull me into sleep and arrive unharmed at my next location.

Michelle Dennedy: There's no Keke challenge for Edna. Edna, the cite for that ISO standard, ISO 20243, is that correct?

Edna Conway: Yes.

Michelle Dennedy: I'm looking forward to the day when ISO 20243 is more popular than 90210. And I think it's coming. It's coming.

Edna, take us home, a quick summary. Where we going to be in five years? Point to the skies, my friend.

Edna Conway: I think we're going to be in a place where we're rapidly approaching now: The new attack surface is going to be functionality. I may get there through your data, but what I'm going to want to do is impact your ability to live, breathe, eat, and to have an enterprise business, and I'm going to affect your brand and your trust if you're a business. I'm going to want to affect the integrity of your citizen's faith in you if you're a government. The way to combat that is a future where we work a better together. We use uniform architectures. We have fewer, fewer standards and fewer guidelines and fewer third parties, only those that are needed. Much as supply chain long ago did when it culled into a lean, efficient model with real needs, real time.

That's where we're going. We've done it before. We've embedded quality successfully. We're going to embed security into our lives every day, every minute.

Michelle Dennedy: I love it. I mean that's the road to trust. Thank you very much, Edna Conway. You can follow Edna on Twitter and I recommend that you do @edna_conway, C-O-N-W-A-Y. She is our chief security officer for global value chain. Thank you so much always for your partnership, Edna, and for helping all of us create this integrated trust model for third parties. We're all a third party to somebody else, right? So, thank you very much for joining the Sigma Riders and, most importantly, for all the great work that you do for our planet. Thank you, Edna.

Edna Conway: Happy to be with you. I'm looking forward to working together in our special 2019.

Michelle Dennedy: Yes. The Year of the Third Party, 2019. You heard it here first, ladies and gents.

So, guys, it's another wrap on the Riders. Thank you very much for joining.

You've been listening to Privacy Sigma Riders, brought to you by the Cisco Security and Trust Organization. Special thanks to Kory Westerhold for our original theme music. Our producers are Susan Borton and David Ball. And a special shout-out and thank you to our Cisco TV production partners. You can find all our episodes on the Cisco Trust Center at cisco.com/go/riders or subscribe wherever you listen to podcasts. And please take a moment to review and rate us on iTunes. To stay ahead of the curve between episodes, consider following us on Facebook, LinkedIn, and Twitter. You can find me, Michelle Dennedy, on Twitter, @mdennedy. Until next time.