Supply Chain Risk Management: Managing Third Party and External Dependency Risk Transcript

Part 1: Why SCRM Is Increasingly Critical

Julia Allen: Welcome to CERT's Podcast Series: Security for Business Leaders. The CERT Division is part of the Software Engineering Institute. We are 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 our podcast website.

My name is Julia Allen. I'm a principal researcher at CERT working on operational resilience. I'm very pleased today to welcome back two of my colleagues, Matt Butkovic and John Haller. Matt is the Technical Manager of CERT's Cybersecurity Assurance team and John is a member of that team.

Today, we'll be discussing a new topic for the podcast series, supply chain risk management. In addition, we'll be talking about a recent symposium that John and Matt hosted on this subject on behalf of CERT. So, Matt, welcome back to the podcast series. Glad to have you.

Matt Butkovic: Glad to be back, Julia.

Julia Allen: And John, I appreciate your joining us today.

John Haller: Julia, thanks for the opportunity. It's good to be back.

Julia Allen: Welcome. So, John, why don't you get things rolling? Just for our listener's benefit, could you describe, when we talk about -- when CERT talks or the community talks about supply chain risk management, what do we mean by that, and a little bit about what you're seeing in terms of why it's becoming more critical these days?

John Haller: Sure. So, supply chain risk management is a term that frequently has different meanings for different people, or for government and private organizations. So, from a cybersecurity perspective, a lot of times, when folks talk about supply chain risk management, they're talking about the integrity of hardware and software, right, like the issue of counterfeits or maliciously tampered items in a supply chain for information and communications technology.

When the financial community, for instance, thinks about supply chain risk management, they're really thinking about third party risk, how to manage and control the risks of relying on third parties frequently for services involving information and communications technology like data hosting, data processing, telecommunications, things like that.

From CERT's perspective, we view the problem broadly and holistically. And we really think about it in terms of external dependencies management. What that means is any situation where your organization has a core service that you offer to your stakeholders or your customers and you rely on third parties or outside entities to support that service with information and communications technology or with services that involve information and communications technology. And that can mean, again, things like data hosting, business relationships that rely on any kind of cyber technology.

As far as why is it a big topic now, it's a big topic for a couple reasons. The first is that recently there have been incidents that have drawn people's attention to the problem of managing third party or external dependency risk. One of them, which is often talked about, is the Target case where Target Corporation had their POS (point of sale) systems essentially that were accessed by criminals through a third party relationship and through a compromise that initially involved a third party and that essentially affected Target's network.

That's one kind of a risk from a third party relationship. There are some other recent incidents. For instance, Department of Defense TRANSCOM (Transportation Command), which is a DoD component that is responsible for logistics, basically moving defense assets around the country and around the world, recently was subjected to a series of incidents involving their contractors where a set of about twenty contractors experienced some compromises, some data compromises that at least potentially affected TRANSCOM's mission. This was actually the subject of a Senate Armed Services Committee report last year that's publicly available.

So, those are some examples of some real world, I think notable, incidents involving external dependencies and external dependency risk. And the second reason I think it's being talked about a lot is that frankly a lot of organizations and a lot of compliance and regulatory agencies or departments are starting to notice that this is a potential area of vulnerability for organizations and something that should, I think, justifiably receive attention in how its managed, right?

So, in the financial community, for instance, the Department of Treasury, OCC, which is the Office of Comptroller of the Currency, last year came out with some updated guidance for financial institutions that stressed the importance of managing third party and external dependency risk. So, I think it's sort of a combination of those two things that really -- has really put the emphasis on it.

And when you think about external dependency risk, it's really kind of a broad subject. And there are other incidents that, to me, are examples of third party or external dependency risk like Havex series of breaches in the electrical industry, which are about a year old now. In one sense, they were what we call watering hole or a drive-by attack. But really it's a -- that series of incidents involved vulnerabilities that stemmed from or resulted from third party relationships. So, it's a pervasive problem that more organizations are paying attention to.

Julia Allen: So, John, and I want to give Matt a chance to weigh in too, would it be fair to say in today's business climate that it's very rare that an organization goes it alone?

It seems like no matter where I look, everybody is in partnership and collaboration, is doing mash ups, is doing acquisitions, is doing some type of business relationship with another either partner, supplier, vendor, subcontractor. Wouldn't you say that's the case? And therefore, this issue really applies to just about everybody.

Matt Butkovic: I would agree, Julia. I think that if you look at the complexity of supply chains, you're right. Organizations are increasingly intertwined. And there's been a move to outsource services such as cloud providers that really bring this issue to the forefront.

John Haller: I think the other thing that's interesting about that is even -- not only do, not only are a lot of services outsourced but a lot of those business relationships change so quickly. And the ways that an organization may be dependent on a third party change so quickly that just keeping up on the cyber security requirements and being able to manage it and know who you're really dependent on can be a challenge.

Part 2: CERT SCRM Symposium; Negotiating Cyber Service Level Agreements

Julia Allen: Got it. Okay, well let's talk a little bit about the event, the symposium that was, in part, the catalyst for our getting together on today's podcast.

So, John, can you tell us a little bit about that event, what it was about, what the objectives were, a little bit about who attended, and any insights that you and Matt gained in conducting it?

John Haller: Our objective was really to bring together some of our stakeholders in the government and in critical infrastructure, both the public and private sector, and really to examine this problem from the different perspectives to see how these problems were similar and different, for instance, between the Department of Defense or between private critical infrastructure organizations -- and to exchange notes about it and best practices, and frankly, for us to learn as much as we could from the community about their challenges in this area.

We were really fortunate. We actually had Terry Halvorsen, who's currently the acting CIO for the Department of Defense, give us our keynote address, which was really great and had a lot of good insight for us. We spent the morning looking at this from the executive or governance level, I would say. And then the afternoon, we took a deeper dive into how organizations are managing the problems and also some of the things that CERT is doing in the area. So, it was good.

Julia Allen: Great, anything you'd like to add about the event, Matt, before I do a little deeper dive on your presentation?

Matt Butkovic: Sure, Julia. I think that the event confirmed for us there's appetite for this discussion -- that organizations are struggling with these challenges. And as John pointed out, there is commonalities between the experience in private industry and in the Department of Defense when it comes to supply chain risk management.

Julia Allen: Great.

John Haller: I'd just like to mention one other thing Julia. One of the things we're trying to do over the next year is we really see the symposium as the start of our department within CERT and certain other parts of CERT in terms of addressing this more broadly. So, we're actually planning a series of activities, podcasts, potentially a webinar, Blog postings over the next 12 months about specific angles or specific aspects of external dependency management.

For instance, we want to look at or have a small outreach activity around managing the risks of relying on software, what you can do as an organization to control that risk. We're also going to be looking at the broader question of dependencies on things like public infrastructure and how organizations can be smarter about that as well. So, we really see this as the first step because we think that it's a problem that will be staying with us and that organizations I think need some help to manage.

Julia Allen: Great, great. So, Matt, let's talk a little bit about some of the topics that you discussed at the symposium. I know in your presentation you specifically addressed cyber service level agreements and their use and their limitations. Could you say a little bit about SLAs and how they're being used today specifically to help mitigate the types of risks we've been discussing?

Matt Butkovic: Sure, Julia. So, SLAs, service level agreements, are a key tool by which parties agree, expectations around a given service. So, they are one way that you can assure that your supplier is meeting expectations and that you're extracting value from that relationship. However it comes with limitations in their ability to protect your organization risk.

One of the things that we highlighted in the event was you can't fundamentally outsource risk. The end of the day the risk falls to your organization. You can indemnify yourself. You can transfer some risk. But true operational risk and financial risk always flow back to the organization acquiring service.

So, we find that many organizations enter into contracts without an understanding of how best to utilize the SLA. They don't write in adequate protections for their organization. They don't monitor the performance of the service provider. And they're often surprised to find that the onus to do things like reporting lapses in service or incidents resides with the consumer of the service, not with the service provider. So, we were attempting in that presentation, to give some guidance regarding how to construct smart SLAs, how to structure a program that best manages your supplier.

Julia Allen: Okay. And I know part of that discussion that you had were some of the key topics. I know you touched on a few but are there some other key topics that you are recommending, based on your work, be included in an effective SLA.

Matt Butkovic: Yes. So an effective SLA requires that both parties understand the specifics of that SLA. We find it's sometimes a one way street -- suppliers writing language that doesn't really provide any sort of flexibility for the consumer service to really adequately monitor or evaluate their performance.

And we find that organizations are often struggling to understand that -- their entitlement to restitution if something bad happens. For instance, there's a famous example of a retailer, an online retailer that on Black Friday had a serious lapse of service and it wrecked their year financially.

But they were entitled to a grand total of three hundred dollars from their service provider because, in essence, no one at that organization had really taken the time to read the specifics of the contract, to understand the SLA and just assumed that there were safeguards built into it. Like any other problem, if you don't have requirements and you don't look at it as an engineered solution, you have little reason to believe that you'll have a positive outcome if left on its own.

Julia Allen: You know as I'm thinking about this and listening to you speak, Matt, I know there are, particularly when it comes to cloud services, there are a lot of big, heavy hitters in the cloud services business, Amazon and organizations like that, who in particular provide IT support and other types of surge services for organizations.

So, does a consumer or does a buyer of those services really have much latitude in negotiating the terms of the SLA with the big providers?

Matt Butkovic: Well, it depends. It depends on scale quite frankly. But you'll find that the large cloud providers will exhibit some flexibility even for middle market customers. So, the stock SLAs and stock contract from all the big cloud providers really leave the customer in a disadvantaged position.

But my advice is there's no harm in trying to negotiate. And focus on the things that are most important to you. We would suggest that those are establishing a way to identify or report incidents, the things that effect your core services. And also, have a very concrete way to seek restitution if something bad happens. Don't leave it to chance.

Part 3: Assessing and Analyzing External Dependency Risk

Julia Allen: Okay. Good advice. Good advice, Matt. Thanks. So, John, let's turn to some of the topics you discussed at the symposium. I know you did a presentation with Ross Geyser of the U.S. Department of Homeland Security (DHS). And in that presentation, you talked about several approaches for more effectively managing external dependencies using a type of assessment, an external dependencies management assessment. Could you say a little bit about that and how it might be used?

John Haller: Sure Julia, I'd be happy to. So, I should mention that the EDM (External Dependencies Management) assessment is based on and derivative of the DHS Cyber Resilience Review that we've been working on with DHS for the past four years as part of our partnership with them.

For the audience's benefit, during the Cyber Resilience Review, representatives of the SEI, along with DHS have visited over 400 hundred critical infrastructure organizations over the course of the last 4 years, basically conducting in-person facilitated assessments of the organizations, the critical infrastructure organization's cybersecurity capability. So, how do they manage, and what do they have in place to manage the problem of cybersecurity across 10 domains? There's actually more information available about that on U.S. CERT website. The EDM assessment specifically is a use of that structure and methodology focused specifically on external dependencies management. So, it's divided into three domains. The first one is relationship formation, forming relationships with external entities, suppliers, vendors, and so forth. How does the organization think about, and does it think about risk at the start of those relationships? Much of that domain or much of that area has to do with what Matt was just talking about -- how do you identify your requirements for the third party and then properly get those into formal agreements, or SLAs, or contracts.

The second domain was relationship management over the course of the relationship. So, there are certain things, for instance, change management, capacity management that in many cases are done cooperatively or with the third party. There's also material in there about how does the organization manage the risk over the course of the relationship. Do they have a process in place to actually become aware of the new requirements as business realities change or as their dependence on an external entity changes?

The last domain is service protection and sustainment. Basically it's looking at your business continuity, service continuity, and incident management processes and capabilities and assessing how well the organization integrates those, and accounts for those external relationships in those activities. So that when, not if, but when there's an actual breach, the organization is -- when there's a breach related to third parties, the organization is better able to handle those and control the consequences of those.

It exists now in pilot phase, which means that it's fully produced but we're looking for organizations to work to assess and to refine the assessment along with. It actually -- the logistics of the assessment are that it's a 4-hour, in-person assessment. It's fully funded by DHS. What that means is it does not cost organizations anything, and we'll go to wherever the organization is, frankly.

And the other really important thing to know about the EDM assessment is that, like the CRR, any organizations -- or any answer or information that an organization provides is protected by PCI. It's Protected Critical Infrastructure Information. It's not used for any other purpose. It's not FOI-able for instance.

People cannot get to it under the Freedom of Information Act. And for any organization that, or for anyone listening to this podcast who would like more information about what that really means, and what PCII is should probably look to DHS. But all the information that we may learn during an assessment is fully protected. It's not distributed or anything like that.

So, I'd really encourage it for organizations. And what you get out of it is you get a good snapshot of what the organization is doing now to manage external dependency risk. And assessments like this really provide a potential path for improvement, being able to visually see how do we manage this now, and are there some places where we can make targeted improvements to become better at it? I think that's really the value.

Julia Allen: Excellent, excellent. Thank you for that summary, John, and giving folks a path to reach out to DHS and your team to engage. So, another thing I wanted to ask you about in your presentation at the symposium was another method that you're in the process of designing or developing called the External Dependency Analysis Method. Can you briefly tell us a bit about that?

John Haller: Sure. So, these two things are complementary. Where the EDM, the actual assessment, looks at an organization's overall capability, the purpose of the analysis method is basically to look at a particular set of vendors that support a particular service within an organization.

So, a lot of times, organizations -- I know this, to some listeners, might sound odd -- but a lot of times some organizations don't even really know who they're dependent on. They know they have a variety of third party organizations. But in a large enterprise, sometimes it's difficult just to identify and to prioritize which external entities or vendors support a particular service.

So, the analysis method, right now, exists in the form of an Excel-based tool. And what it does is it solicits from the user information about the key services that the organization provides. Then it guides the user to identify the specific third party suppliers or vendors that support that service. And then what it does is it asks a series of questions for each third party or supplier about what the organization does to actually manage that third party dependency.

The questions themselves -- it's pretty lightweight. It's like -- it's fifteen questions or so per third party or per external dependency. The questions themselves are drawn on resources like the CERT Resilience Management Model, the DHS Cyber Resilience Review, the EDM assessment itself. And they're also somewhat influenced by the recently released NIST Cyber Security Framework. So, that's where the questions come from.

The output of the tool is -- it actually builds a chart or a graphic that shows the user, that shows the organization, the third parties that they rely on to support a specific capability or service, right? It provides an impact ranking of those. And then it charts that against what the organization really does to, what the organization does across those categories to manage the dependency. And the idea is that if you can have a visual, you can hopefully make good, repeatable decisions and actually, frankly, use it as a management tool with leaders and managers within the organizations to track some of these dependencies and to make smart decisions, right? Security budgets are limited. So, if you can have some way to, in a repeatable, easy -- well, relatively easy way to see some of these dependencies and make smarter decisions, then you can use your security dollars a little bit more effectively and efficiently. That's the basic idea. That's really the idea behind the EDA method.

Julia Allen: Great. And Matt, anything you wanted to add to what John's been describing before we move on?

Matt Butkovic: Sure. I'd say, Julia, that we've designed all these things to be as practical as possible, understanding that organizations typically can't spend days or weeks on these problems in the form that we've created. So, the focus is really on usability, affordability, and making it as light a lift as possible for organizations to learn these things about the critical dependencies in their supply chain.

Part 4: Addressing SCRM for the U.S. Department of Defense

Julia Allen: Great. So, John and Matt, just a couple of more questions for you before we come to our close. I know, John, that we've been involved working with the critical infrastructure protection sector for a very long time, including this work. And a lot of that are based on private/public partnerships. And a lot of the control for those types of services are held in the private sector.

So, how do we make this body of work applicable for our primary sponsor, the U.S. Department of Defense?

John Haller: Well, we've actually been talking to a couple of DoD entities about that. So, one of the interesting things about these methods, and it traces back to the lineage and descent from the CERT Resilience Management Model.

When we -- and as Matt, and I think I, have indicated, we do a lot of work with private critical infrastructure, right? When we identify a service within private critical infrastructure, that, and then look at the cyber resilience behind that and capability to support that service, that is very similar and very usable in a defense environment as well.

Where, for instance, in a financial institution, a critical service might look something like clearing and settlement, mortgage financing, money transfers using the SWIFT system or something like that. In a military organization, a critical service or a critical mission capability might look something like anti-submarine warfare, ground transportation of military assets, something like that, right?

In each case, they're mission critical capabilities that are supported by cyber, supported by information and communications technology. And we think there's a lot of applicability between what we're doing in the private sector -- or, I should say, in critical infrastructure, and some of the problems that the military has in certain cyber security areas.

So, right now, we're actively looking for DoD organizations, departments, and agencies to work with and to expose some of these tools to them and then get their input and feedback as well and to explore that question further. But I think that, to make a long winded story short, it's directly applicable. And I think a lot of these problems are more similar than different.

Julia Allen: Well, and also, you get to the fundamental foundational services like electricity and communications and transportation. The DoD is just as dependent on those as a private sector enterprise, right?

John Haller: That's right.

Matt Butkovic: Absolutely.

John Haller: That's right.

Julia Allen: Anything to add Matt?

Matt Butkovic: No, I think that John's really hit the highlights there which is we believe these problems are -- that is the challenges of the DoD and the challenges of private critical infrastructure are more similar than dissimilar.

And I would also highlight the increased integration between the two where you have commercial providers of IT services enter into large scale relationship with the DoD to provide things like cloud services. So, I think that in the future, as these things become more and more closely aligned, we'll see that this convergence requires us to have a common set of practices for managing supply chain risk.

Julia Allen: Great, great. Well, John and then Matt, do you have some places where interested listeners can learn more of this critical subject?

John Haller: Sure, Julia. I think that the show notes for this podcast will include PDF versions of the presentations that we provided at the symposium last month in January. They will also include links to the Cyber Resilience Review and to the DHS site that talks about the Cyber Resilience Review.

Julia Allen: Okay, and Matt, I know you've been doing some blogging and some webinars. Did you want to highlight those before we wrap up?

Matt Butkovic: Yes, certainly, Julia. So, in advance of the symposium, we did a webinar where we did a deep dive on all of these topics. So, there will soon be a page on the CERT web presence where we'll have links and all of these resources available to the listeners. So, the symposium notes, the webinar in its entirety, and some blog content and other links to resources.

Julia Allen: Great. So, first of all, Matt, let me thank you for your attention and preparation today and your leadership on this very important subject. Glad to have you with us today.

Matt Butkovic: Well, thank you, Julia for facilitating the podcast.

Julia Allen: And, John, again, I know that you're really leading the charge on a lot of this work. So, thank you for making it available to our podcast listeners.

John Haller: That's my pleasure.