SEI Webcast

How I Learned to Stop Worrying and Love SLAs

by Matt Butkovic and Alan Levine

Shane McGraw: Hello, and welcome to today's SEI Webcast, "How I learned to stop worrying and love SLAs." My name is Shane McGraw, Outreach Team Lead here at the Software Engineering Institute, and I'd like to thank you for attending. We want to make today as interactive as possible. We will address questions throughout today's presentation. And you can submit those questions in the YouTube chat area and we will get to as many as we can. Our featured speakers today are Matthew Butkovic and Alan Levine. Matt is the Technical Director of the Risk and Resilience Team within the CERT Division here at the SEI, where he performs critical infrastructure protection research and develops methods, tools and techniques for evaluating capabilities and managing risk. Alan is a former Chief Information Security Officer for two Fortune 500s, Alcoa and Arconic, where he held global accountability for all aspects of cybersecurity, data privacy and protection, IT compliance and eDiscovery for 20 years. Now I'd like to turn it over the Matt Butcovik. Matt, good afternoon, all yours!

Matt Butkovic: Okay, thank you, Shane, and Alan, welcome! So, glad you could join me. So, first I want to talk about the title. I think maybe it's a bit of a stretch. We're not going to stop worrying, but maybe we'll worry less if we're using Service Level Agreements. And I know on the surface, this sounds like a relatively dull topic, but I think you'd agree with me, this is an absolutely critical element of managing third-party relationships. So, with that said, I thought Alan, we could start with a bit of a history lesson and then explain why SLAs are vitally important today. So, this first picture, right? And many people will guess this is Pittsburgh in the photo, it's not. You can tell because it's too flat. This is actually Ford's River Rouge plant in 1927. And though I'm a native Pittsburgher and I love photos of old industrial stuff, I'm not showing you the picture just because it's old industrial stuff. And it's interesting, but rather it's the exemplar of something. At the time Ford was the model of vertical integration. Ford rolled its own steel, pressed its own body shells, stuffed its own leather seats with horsehair, rolled its own glass, generated its own power, had its own railroad, had its own fire department, had its own post office, was all contained in this site. And every 48 seconds, a Model A or a Model T rolled off the production line. This is not the enterprise that Alan knew as a CISO, and it's not the enterprise you work in today. But for lots of very good reasons, we've moved away from this very centralized way of working to a decentralized way of working that requires elaborate complex relationships with other organizations. So, Alan, maybe just to kick off here before we get to the next slide. Is it fair to say that in your experience we've seen this progressive reduction in the hands-on entity direct line of site relationships and organizations? Depending on third parties more and more?

Alan Levine: Yeah, I would agree completely. And it's happened not just in IT, it's happened across the board in large and medium and in some cases even SMBs, right, small businesses, where folks have made the following choices. They've said, a) "I don't have the resources, I can't afford the ON and FTEs, in other words, the quote/unquote "employees" to do it and so maybe I will find somebody else to do it."

So, that's one reason. Another one is some organizations decided that they wanted best of breed, and they weren't incapable of doing best, and so they looked to a third party that might be able to provide best, if not better than what they were capable of doing internally. And I think there's a third reason that is endemic more to IT than anything else, and that's the shrinkage in terms of the available labor force. In other words, can you go out and get talent to do the job inside your organization? The motivations that move an organization to a cloud, whether it's just for Exchange email to 365, or whether it's more Infrastructure as a Service, Software as a Service where organizations are making conscious decisions to shrink what they have inside, and embrace what's available on the outside through services.

Matt Butkovic: Yeah, thanks, Alan, I think that your experience mirrors my experience when I was in private industry. And you're absolutely right. This is not-- it's not an IT specific or IT only situation, right? The depth and breadth of outsourcing and third-party reliance cuts across all lines and all functions within an organization. So, on the next slide to compare and contrast yesterday's enterprise, the Ford example in 1927 with a more contemporary example. So, this is Boeing's 787 Dream Line. And I know we have a number of folks joining us from international location, so welcome the audience participants from Canada and Switzerland and Mexico. You'll notice on this slide, that there are pieces of this airliner coming from every inhabited _____ 00:06:02. So, think about the complexity in supply chains. And these are only major components. And so, Alan, your old organization was responsible for creating many of the pieces' parts on this graphic. I think it's also fair to say that the major components listed here, let's say Alcoa was building a section of a wing, or a part of an engine, there was a complex ecosystem of smaller vendors underpinning that component, correct?

Alan Levine: Oh, absolutely. I mean, for every widget that we made, most of them were larger widgets, there was an almost endless stream of suppliers and sub-suppliers and sub-sub-suppliers that were making individual discrete parts for that widget. And then part of our job was to take all of those individual discrete parts and put them together, so that we could make the widget, or in some cases, let's say the form for an airplane wing, or the fan blade for an engine, in order to move it on to the next stage where Boeing could find them all the parts compatible and put them all together. Yeah, it was an almost endless supply chain.

Matt Butkovic: Yeah, and all of that, that endless supply chain, or sometimes report as the fourth-party problem, and all of that inter-- it's all underpinned and the interconnectiveness of that is electronic these days. So, there's a vast digital network, a skeleton, if you will, that connects all of these things. So, there's a question here from the audience which is, "How does cybersecurity SLAs different from other SLAs?" and we'll get to that in a minute but if you think about the SLAs that are required to do what this diagram depicts, which is bring all these pieces together. There's a specific understanding of the thing you're making, the quantity in which you're making it, and when it'll be delivered for assembly, right? So, that's

one type of SLA. The SLAs that Alan and I are most familiar with are SLAs related to the security performance of an organization. So, in concept, I would say they're not that different, right? A Service Level Agreement in any facet of the business is a specific documented understanding between parties regarding the delivery of a specific service or the production of a specific good. The difference I would draw our attention to and Alan, I'd like your thoughts on this, in our profession, we are most often then needing to apply the overlay of how well did you perform a specific task in relation to criteria we presented? So, it's not in concept that different from the manufacturing spec, except for in manufacturing, you're not subject to as many variables. What I mean is there aren't thread actors trying to thwart manufacturing as readily in most cases. Is that fair, Alan?

Alan Levine: Yeah, I think that's fair. You know, I think we have to break down this notion of an SLA into the three natural parts.

Matt Butkovic: Yes.

Alan Levine: Well, you have Service, you have Level and you have Agreement. So, let's take them one at a time. The first one, Service, assumes not that you're receiving a product, but that you're asking someone, a third party to do something for your organization. Something that maybe you decided consciously not to do and have wanted to outsource. Maybe it's something you could never do, it's above and beyond your capability and a third party has come up with some secret sauce to give you a service you never even envisioned. Maybe it's because you simply want to focus your organization from the CEO and Chairman down on business value and business drivers, and doing the, you know, deciding who's going to run a help desk is simply not a business driver, and so you've looked to a third party to provide that. So, that's a definition of service. What is the thing you're going to a third party to get? By the way, if we put IT aside and we go back to that original thought of, "Well, this didn't begin with IT," you know, what was the first service that most large organizations decided to move to third parties as a service? It was probably janitorial service.

Matt Butkovic: Right, exactly! <laughs>

Alan Levine: Say, "I'm just going to hire somebody else to clean up." Now that brings us to the second letter in SLA, which is the L, Level. So, Service *Level* Agreement. So, when you think about the level, well, if it were janitorial services, it was essentially a Yes or a No. Is it clean, or isn't it clean? And that was the definition of the level of service you expected. So, then we're going to delivery janitorial services, and you expected everything at the end of the day to be clean. In terms of IT level of service, it's obviously much more complicated than that. And that's why SLAs that are well-written are founded in a request, a sincere request for honest and regular metrics so that the per-- the organization that is requesting and

receiving the service understands what is expected by the service provider. Now that brings us to the third letter, Agreement. What you believe you're going to receive in terms of a service may not always be what you end up getting as a service. At all times, when you're requesting a service, and you're willing to document it in an SLA which is a contract, you want to be able to say, "We, the supplier of the service; and us, this is the folks who are going to receive the service, our organization, agree that these are the services we expect, and these are the levels we expect with the metrics for how we will measure those levels." If either party is reluctant or hesitant to agree to the S and the L, then you're probably not going to end up with an A.

Matt Butkovic: That is an excellent unpacking of SLAs, Alan. So, in your description, I think there's a few attributes I draw our attention to. But in conversation, let's pivot now from speaking broadly about SLAs, and speak in greater detail about cybersecurity SLAs, or security SLAs. So, and what I'm about to say is applicable to all types of SLAs, but in our context, these are, I think, the key attributes. You mentioned clarity. Both parties must sincerely understand what's being asked of them, right? So, you can't have an expectation without some articulation of the specific something you intended to have. Specificity. The details really matter, don't they, Alan, in SLA?

Alan Levine: Right.

Matt Butkovic: You're going to live and die by those details. And then I think, arguably, most importantly, you described measurement and enforceability. If your SLA doesn't provide you with a monitor of the performance, and the means to apply correction to the performance of the supplier, then really your SLA has failed, right? So, in a minute here, I'd like to kind of pivot to what makes a good SLA. But, Alan, I'd like to take a slight detour. So, on this slide, and just, to me, this is visually a very interesting photo. So, this is an IBM data center in Montreal in the mid-1960s. Now, you and I know it's bad operational security to have a data center that looks this way. The truth is you never would, right? But why use this photo? So, to me, it captures what we want in our service provider, which is this couple standing on a sidewalk, and they're looking in on this mainframe operation. At any time, they can see what's going on. And there's an operator there at the terminal, let's call him Chuck. They could politely tap on the glass and say, "Chuck, we'd like to know what's going on? Can you tell us which process you're running?" and Chuck would point to the run book. Well, you and I know this isn't what third-party relationships look like. You don't have ubiquitous visibility into the operations of the third party, right?

Alan Levine: Right.

Matt Butkovic: So, let me just pause there for a second, Alan.

Alan Levine: Yeah, and in fact, that's the first thing you lose.

Matt Butkovic: Yeah.

Alan Levine: So, you know, when you decide to have someone else provide a service for you, you lose the ability in most cases to see indeed in very great detail how they're providing the service. You know, do they have to kill 17 dogs every day in order to provide the service? You may not know that. If you knew, you might be very upset and say, "Well, that's not the service I signed up for. That wasn't what we agreed to." And the service provider might say, "Well, you never said, "No" to killing dogs." That's why the agreement is so important.

Matt Butkovic: Right.

Alan Levine: It's emphatically clear that in addition to losing visibility, you lose hands-on control.

Matt Butkovic: Right.

Alan Levine: So, someone else is providing the service, you're not doing it. When it comes to cybersecurity the notion that you, your CISO, your CISOs organization are not doing cybersecurity, but are essentially managing a contract that has someone else doing cybersecurity for you. For many CISOs and CISO organizations that by itself is a leap too far to have somebody else do it. However, if you can say, "Well, they're going to do it, but I'm going to have full visibility. That window is going to be completely clear! We're going to use Windex cleaner on it five times an hour to make sure that you can see *everything* that's happening inside that room," well, then the CISO and the CISO's organization might feel better about not doing it themselves, because they can see exactly how it's happening and they can notice whether or not dogs are being killed. Right? And stop the presses immediately.

Matt Butkovic: Yeah, and Alan, I think you're spot-on, that you're trading visibility. You're consenting to operate in a moral paveway [ph?] for lots of good reasons, right? There's costs, or there's access to the right labor. All those things are very important. But it is a choice. And that choice comes with certain consequences. Right?

Alan Levine: Mm hm.

Matt Butkovic: So, let me just pause for a second and lay out one of the tenants, I know you and I are absolutely committed to conveying to the group, which is these organizations that you contract with are an extension of your organization in cybersecurity, right? They are another tendril of your organization.

Alan Levine: Mm hm.

Matt Butkovic: And if you treat them simply as an entity that sends you an invoice, that you don't have to worry about, right, you can find yourself in a very difficult situation.

Alan Levine: Right, right.

Matt Butkovic: So, this situation of third-party management, third-party risk management comes with its own skillset. It requires its own skillset. And chief among those skills is understanding how Service Level Agreements are the primary mechanism by which you'll govern these relationships.

Alan Levine: Right.

Matt Butkovic: So, on the next slide, this is just-- this might seem a bit remedial for some folks, but this is a definition from iTel of what a Service Level Agreement is. Now, Alan and I aren't going to read the slide, but I want to draw your attention to how it reinforces the things we said earlier, right? That an SLA needs to be documented. If someone says they have an SLA, but it is ad hoc, not written down, casual-- you don't really have an SLA. Right? It has to be written in a specific form, which again, it clearly articulates what's expected and articulates the measures. And these things will exist in that larger contract that you have with the third party. So, it seems like I'm belaboring the definition here, but there's a reason behind this. Especially in cloud relationships, and I would argue cloud computing has been one of the most transformative technologies we've seen, at least I've seen in my time in IT, and IT security. This is the primary mechanism by which you will not only measure success and failure, but the primary mechanism by which you'll incent and change behavior in a third party. So, Alan, just let me pause there for a second. I think definitionally, right, we could pick other definitions of SLAs, but I just want to reinforce with the audience that we should draw on the collective wisdom here. This definition applies for cybersecurity SLAs as much as it does for SLAs related to the manufacturing of widgets, right?

Alan Levine: Oh, it absolutely does. And I think because we have this definition up on the screen, I think it's important to reinforce that a CISO or a CIO that's making these decisions should not be the person that's doing the final review on the SLA. This is a contract between the customer, the recipient of the service, and the provider. And I think it's cri-- and in most organizations you'll have procurement folks in the middle of this, because they are the people who establish and govern the relationship with suppliers. You know, they buy the stuff for an organization, including stuff meaning services, but you know, the constituency you should not avoid in all cases is your lawyers, your attorneys. Because this SLA is, as I said a moment ago, a contract. And it's a contract between your organization, your company, your

enterprise and a third party that's going to provide one or more services. And so, I can't emphasize enough that to have legalize on the legalese that's inside this agreement is imperative.

Matt Butkovic: That's great, Alan, and I think it's also the case that we have to readily admit the limits of our knowledge and skills. So, the only thing worse than an attorney playing CISO, is a CISO playing attorney.

Alan Levine: Exactly! <laughs>

Matt Butkovic: So, this is truly collaborative, working with your law department, your contracts folks. My experience was that the law department knew how to execute. They knew how to find the right mechanism to get what we needed. But they didn't know, as you might suspect what the terms meant. The contracts folks were very adept at creating the contract vehicle, but again, they were building a container, and the contents of the container were up to us. So, if these three pieces aren't working in unison, you really are not deriving value from your SLAs like you should.

Alan Levine: Right. Yeah, I mean, to coin a phrase, "It takes a village," right. It's going to take a bunch of different people, constituencies within your organization. If it's an IT service, cybersecurity or otherwise, obviously your CIO and your CISO, your procurement folks, as I said, who manage the supplier relationship, your legal folks who will make sure that your organization is protected. And that the organization is providing the service is doing those things you expect and not doing those things that you don't expect. For example, killing 17 dogs. Right? The lawyer will make sure that the language in the SLA says, "No dogs will be harmed in the performance of this service," if that's what your organization decides is the proper position to take in the agreement.

Matt Butkovic: Yeah, thanks, Alan. So, there's a few questions here from the audience about another piece of that village that it takes to effectively use SLAs. And that's the audit mechanism or the review mechanism. So, let me offer this straightaway, and I think you'd agree, Alan. I know you'd agree. Don't bother creating SLAs if you're not going to do performance management with the vendor. So, if you're not capable or not willing to get performance data that allows you to determine if that third party is meeting the terms of the SLA, you're really kind of wasting your time. And moreover, you might be creating a false sense of safety. So, auditing these relationships, reviewing performance-- and I'd also say, if you're only doing that at contract renewal, you're doing it wrong. That is not the way to look at this, right?

Alan Levine: Right!

Matt Butkovic: So, let me stop there, Alan. In your experience, any tips for the audience regarding how-- both how you best ensure you're getting timely and accurate information back from that third party that is responding to your SLA?

Alan Levine: Well, what I would recommend, wherever it's feasible, is to include all of that detail inside the SLA to say, "Our expectation as the customer, as the recipient of the service, is that we're going to receive these metrics on an hourly basis, a daily basis, a monthly basis, a quarterly basis. And that any failure to provide those metrics with the quality we expected, the detail we expected and within the timeframes we expected-- any variation from that is a violation of the Service Level Agreement." You might say, "Well, sometimes you get into a service level relationship and you don't know what you *should* expect." Well, that's the moment to step back. Don't sign any SLAs quite yet. Because if you're entering into an agreement for a service where you're not sure what you should expect, then you shouldn't be signing the agreement. The service provider will have a list. They will say, "Well, these, you know, this is our menu, this is the stuff we normally give you, and by the way, some of it may come with a price. Oh, you want *hourly* updates in terms of metrics for performance, well, we can certainly give you that, but we're going to have to hire two people to do that, and so that's going to be an additional cost above and beyond whatever is agreed to in our relationship." They may say, "You know, we don't vary," especially if it's the largest cloud providers, they're likely going to say, "Here's what we offer. And that's all we offer. You may want something different, but we can't provide it." Until you, as the recipient of the service, the customer organization understands explicitly what you believe you will need in order to define, well, maybe in order to identify success in terms of that service delivery, you shouldn't be signing the agreement.

Matt Butkovic: I would agree, Alan. And it's easy, especially for organizations that aren't as familiar with these contract vehicles to be sort of fault-- lured into accepting the easy, but relatively meaningless SLAs, right? Availability metrics are easy! Right? That's table stakes. Doing good security metrics, that's hard. Right? So, there's a comment here from the audience, I think it's very important as well. As part of that overall set of things you're going to think about in SLA is where the service will be delivered from. Right? So, let's kind of pivot our conversation now. We'll talk more specifically about the cloud. You mentioned the cloud, right? Which I think is one of the more difficult SLA situations for us. The premise of the cloud is that you have ubiquitous access to a fungible pool of resources. That doesn't mean it's on the-- in the data center on the street corner in Montreal and you can look inside, right? In fact, it's on many corners all over the world. You may not know at any one time. If you have a specific obligation, regulatory obligation or need, then I would argue this about best practice, you need to specify where that data's going to live. You have to understand your SLA, and make that part of an SLA, right? We will ensure that our data remains within this specific fenced set of data centers. So, Alan, I can think of an example from my past, but any thoughts there about examples from your past regarding that--

Alan Levine: Yeah. Certainly, a lot of, you know, predominantly the answer to that question today would be based on GDPR. I think we all understand that, right? So, that, you know, there are lots of cloud providers who have created an instance, in Ireland, for example, because it's from Ireland that they're going to provide the service. They now remain inside the quote/unquote "union" and so they believe that helps to solve the quote/unquote "GDPR problem." But there are other issues, right? I mean, data comes in a variety of forms. And sensitive data, even in *more* varieties. So, you have PII, Personally Identifiable Information, and that's certainly the focus of legislation and regulation like GDPR, but you also have in the United States a strict concern for Critical Unclassified Information, CUI. And restrictions, not necessarily on who can view, but on how well that information will be protected. What level of security will be applied to data protection for CUI. Same could be true for health information in the United States via HIPAA, and other various parts of the world. So, first, you need to define what is it that we're trying to manage? What is it that we care about? And then get to the point where you feel comfortable outsourcing that, the management of that thing you care about. Because you may stop at first base, to use a baseball analogy, and say, "You know, I can't get any further, because I care too much about that to give it to a third party to manage on my behalf. I can't do it. My conscience won't let me. My regulations won't let me. My boss won't let me move it to a third party. I'm going to need to figure out a way to manage it myself." If you're able to make the leap, and in some organizations it's a leap because of GDPR and because of concerns about PII, PHI, CUI and other sensitive information, if you're able to make the leap that you can have a third party manage that information, now you have to go to the next level, which is, "Okay, how well are they going to manage it? What is going to be my evidence, my proof that they are managing it to the regulation and just as importantly, to my expectations as a customer for protecting the data?"

Matt Butkovic: Yeah, that's a great point, Alan. And you know something really interesting, it's probably underexplored in this topic, if your organization today, prior to outsourcing, doesn't know what the critical assets are, where they live and how they're going to be protected, you really aren't ready to do this.

Alan Levine: Mm hm.

Matt Butkovic: Because there's no way to sensibly articulate an SLA, if you don't know what the requirements are internally to start with.

Alan Levine: Right.

Matt Butkovic: So, I would argue all of this is predicated on a policy set and governance. It doesn't have to be complicated. You know, one of the common refrains is, "Well, what about small and medium businesses?" The truth is, yes, it could be more difficult if your resources are more constrained, but this isn't beyond any organization of any size, right? Is that--

Alan Levine: Right, and theoretically, Matt-- and I'm sorry to interrupt-- theoretically, you know, I hear a lot from SMBs that, "Well, you know, it's a bridge too far to do this kind of data identification, data classification, data protection in order to determine what we could have a third party handle for us. By the way not just data but the applications from databases and infrastructure that manage that data as well. That's all relative concerns within the data pocket, right? What I would say is if you're an SMB, a small business you probably have less data to worry about also. You know, you don't have millions of files. Maybe you have thousands of files and so yeah, you have fewer resources you can put toward the question, at least to get an answer to the question, but you also have less-- theoretically less data that you need to sort through in order to do that identification and classification, in order to establish what you believe are the rules of the road for protecting that information so that when you move it to a third party you can ensure that they commit via the SLA to that same level of protection as a minimum, that is the cost of entry.

Matt Butkovic: Yeah, absolutely agreed, Alan. One of the things that worries me is that AC organizations, especially small and medium-sized, they have this kind of Faustian bargain where as part of the outsourcing, they eliminate the very resources required to sensibly manage these relationships.

Alan Levine: That's right. Yeah, you know, I know nothing I see nothing you just take it from me and hopefully nothing goes bump in the night. That's not what I call an SLA. That is not an agreement that is a wish. That's a silent prayer. That is not the way we do business.

Matt Butkovic: Right. Hope is not a strategy, right?

Alan Levine: Exactly right.

Matt Butkovic: And so I want to pivot the conversation slightly. So we're going to talk more explicitly about the cloud, and SLAs, developing SLAs in the cloud and forcing oversight in the cloud's a very difficult subject. However you need to do it, right? And this is an absolute essential part of utilizing cloud services. So imagine if we will, right, we've gone from the data center we can look into any time and see what's going on to, we're looking through a keyhole. And what we're going to do with the SLA is determine the specific dimensions of the keyhole, and the lighting in the room. Now one of the one of the things that you often will need to give up on is the idea you can independently verify what a vendor is doing especially in cloud relationships, your right to audit clause if you will. So in another webinar, we'll tackle sock reports and third-party attestation, but for today I just want to stay on the topic of SLAs and contracts. So on this slide we're going to explore a unnegotiated stock cloud SLA, in cyber security, SLA. So this is a Google example. Don't worry, we'll pick on others. This is just our starting point. And it

reads, each party will protect the other party's confidential information with the same standard of a care it uses for its own information. Now do we see a problem with this, Alan?

Alan Levine: Absolutely, my head's about to explode, you know. I mean the fact is that you're, as a consuming organization the, consumer of a service, you're now saying, whatever you do for your information as a supplier is good enough for me. Well what if the supplier doesn't have any PII, PHI, CUI? What if they don't have to worry about GDPR? What if they don't have to worry about CCPA? I mean the fact is, it's your data and you want it managed to a standard of care that you as the consuming organization define. The problem is most large cloud providers aren't going to give you that option necessarily, and here's an example. You know, what this says is, we as the provider are going to treat your data as well or dash, dash, dash, as poorly as we treat our own data and you should be happy with that. Because if we treat your data as poorly as we treat our own, well, you know, the lowering tide will sink all the boats at the same time.

Matt Butkovic: Yeah absolutely. So this is one of those phrases that on the surface you might say, okay well, there's an equivalency here. This is really important for us that I'm a small business. Google's this enormous enterprise where everyone trusts Google. This must be okay. The truth is, this statement's not okay. You must examine what this means and this is-- just to be clear, we're not suggesting you not use these services. We're suggesting you become informed or more informed consumers of these services and understand the risk decisions implicit knowledge.

Alan Levine: That's right, and I understand why cloud providers want to include statements like this. So they may have one security regime, so that means one set of standards and practices, one set of policies, one set of personnel that are securing the entire organization, meaning the provider's own organization and those partitions or places where they are now managing customer data and customers, and providing customer services. So if they can do that all with one team from one virtual place, I could see the benefits for the provider. However, as I said earlier, I also see the problems for the recipient of the service, because they are left with two problems. One, they're left with the notion that their security for their stuff in that cloud environment is only going to be as good as the provider provides for its own data. And then two, of course, I think this will lead us naturally to a place where there's not going to be a response to our request for visibility, because the provider is going to say, "Well I told, you know, I'm doing for your data the same as I do for my organization itself, and I would never tell anybody what I do for my organization itself to protect my data. So I've just closed the door on any ability for you to have visibility into what I'm actually doing with your data."

Matt Butkovic: Yeah.

Alan Levine: Right. It works. It works really well for the provider.

Matt Butkovic: Right. So before we find our Gmail accounts have been terminated--

Alan Levine: Mine already has while we were talking.

Matt Butkovic: -- I want to think of another example, Alan. And this is the Amazon example. So this is a variation on a theme for us, right? So there's references to reasonable and appropriate measures, never specified.

Alan Levine: Right.

Matt Butkovic: I think this is really-- the next line is the one that trips up a lot of a lot of organizations with limited knowledge, right. You the organization are responsible for configuring and using the service offering, and taking your own steps to maintain appropriate security. Well, wait a minute. I just went to the cloud because I can't do those things, right? I don't have the people to do those things. It's on you, so there is no default setting that says you are secure and you're paying for it without examining the specifics here.

Alan Levine: Right, and there's one more, you know. It's the limitations on liability. It's not just that Amazon's not responsible for damage, and I'm not picking on Amazon here. I think this is a fairly constant mantra among cloud providers, is that they totally eschew third-party liability. So what is third-party liability when it comes to cloud SLAs? The example would be, so you have a relationship with the cloud provider and you're both-- imagine you're both human beings walking down the street. You might be walking hand in hand because you have an agreement where the cloud provider is providing you with a service. You're walking down the street, a mother comes by and bops you in the head. And as you fall, you take out the cloud provider, the buddy that you're walking with. You both land hard. However the cloud provider lands hard inexplicably, as far as they're concerned, because based on the eschewing third-party liability, they would say that wasn't the mugger's fault. That was your fault as the customer for landing on me. So what does that mean in real life? Well, it means this is the position of most cloud providers, that your security as a recipient organization, is what we will count on as a provider, and if a third party, a hacker-- let's just use somebody dark today, okay? Yes, those folks who have damaged the pipeline or at least force the pipeline to close.

Matt Butkovic: The Russian action group, yeah.

Alan Levine: Yeah, so let's say that they attack your organization. This is the customer organization, the recipient organization, your organization. They attack your organization and then through that attack are

able to launch something malicious or nefarious against the cloud provider because of the network connection, because of the fact that you are storing data and apps, and maybe infrastructure out there, that through that pipeline the bad guy essentially uses you as a launching point for an attack against the cloud provider. What all of these SLAs, cloud SLAs say is that it they don't care that you've been hacked. They only care that you will be accountable as the customer for any damage to the cloud environment, not the hacker. That's on you, because your security wasn't good enough to keep the hacker out, and so that is this whole point of eschewing third-party liability. They have no interest in going after the hacker. You as the customer can't raise your hands in the air and say, "Well, you know, they took advantage of me and so through that took advantage of you. I'm sorry." Sorry won't cut it in terms of this relationship. If there's damage to the cloud provider, they will be coming back to you to claim those damages.

Matt Butkovic: Yeah. Alan, I think this is sometimes-- I mean often misunderstood, and your description or your analogy of the mugging, many organizations don't understand that it's up to you to identify there's been a mugging. Unless your contract reads that they are-- that the service provider is to alert you, determining that service outage is up to you, right? So that-- let's kind of recap where we are. So we know that in in cloud SLAs you're not going to have the standard level of visibility that you have in your own organization, right? You're not likely going to have a solid mechanism to do third party independent evaluation of the cloud provider, right? You're going to depend on some attestation done by another. We know that there is no equivalency in security policy. If I have a provision that says I do x. there's no reason to believe Google's going to do that, right? So here's where the story gets a little worse. So what are your auditors, your examiners expecting, right? So I pulled this from the ISACA [ph?] guide to auditing outsourced services. Early in my career, I was a full-time IT auditor. We used to turn to these sorts of things for guidance for our programs. So I think this is worth exploring in a little detail. If your examiners or auditors are using this kind of guidance, they're expecting to see that the third party has an equivalency between your policies and their policies, and that they're proactively alerting you when something goes wrong. Well, we know by reading the SLAs and the contracts, this isn't what you're buying. So to paint a fairly bleak picture, here's things you can't get and then the auditor is expecting to see the very things you cannot obtain.

Alan Levine: Right.

Matt Butkovic: So, Alan, thoughts about this? Do you ever find yourself in this situation?

Alan Levine: Yes. I can't, for obvious reasons because it was audit-related, go into the specific details, but I'll say so first, we're making an assumption that the SLA, or the master agreement that sits above it, includes a right to audit, and it may not, especially with cloud providers that we were speaking about a moment ago. In many cases you will ask for a right to audit, you won't get it. You might say, that by itself

is a deal breaker. Well, you also want to talk to your own folks, because clearly for the folks who supply to you in the marketplace, all those people in the supply chain that we talked about early on in this presentation, you know, you've tried to impose a right to audit on all of them and a bunch of probably rejected it. Some have probably accepted it. So it's not unusual that your providers, your suppliers in the in the cloud space and elsewhere in the services space, would deny you a right to audit. Let's say they accept it and say, "Okay, we'll let you do an audit." The next question any auditor is always going to need to answer is, what am I auditing to? Am I auditing to ISO? Am I auditing to NIST 171? Or am I auditing to my company's-- this is the service recipients company-- am I auditing to my company's standards, my company's policy? Let me give you an example. As an auditor within my organization, I am aware that because of cyber security concerns, the organization uses privileged access management and privileged identity management PIM PAM, to say all of the IT administrators within my organization are required to go to a vault to check out their privileges. It uses multi-factor authentication to control who can get those privileges. It cancels and checks back in those credentials after a short period of time so that they don't linger out there dangerously. Fine. I as the auditor now understand that. I go to the third party and I realize, if I can even get this visibility, that their IT administrators-- this is the provider organization, not a provider of the service-- that they don't use PIM PAM. Well, do I write them up for that? Because we use it and the provider doesn't? That's one example. It could be something as basic as the strength of a password for users, right, where in our environment it's x and in their environment it's something less than x, in terms of strength. I think it puts the auditor in a position where even if we have the right to audit and even if the order can get the visibility that we talked about earlier, that they may be met with disappointment right? They may find that, you know, what we do here is not what they do there. What's the next step? Go back to the agreement, the SLA. What did the provider commit to do in this regard? That's the question the auditor will have to answer.

Matt Butkovic: Yeah, thanks, Alan. You make a really good point. So just to maybe state the obvious, but it's certainly worth stating in this context, you can't fundamentally outsource risk. You can transfer risk, you can try to indemnify your yourself against risk, but the risk that you bear will be disproportional, meaning the service consumer is going to shoulder a far greater portion of the negative outcome than the provider. That is just a fact. But you often will then hear, "Well, but we're entitled to some compensation or restitution if something goes wrong." So on this slide, just a quick summary of what you're actually entitled to. And for the sake of time, you can come to the summary view on this. You are not entitled to damages. You don't get, unless your contract says it. Your SLA doesn't say that you're going to be made whole when you experience a loss. So if you're in e-commerce and your site goes down at the peak of sales season, you're not entitled to some liquidated damages or some other settlement. You're typically entitled to a service credit. So you get more of the service that just failed you, right? Also, as we said, it's up to you to file, and most of these agreements. it is up to you to let the service provider know something bad has happened and then they're going to give you a service credit. Now that should leave you a bit

cold, right? Again we're not saying-- Alan and Matt are absolute advocates for using the services. Just use them in a smart way. All of what I've just described needs to go into your risk calculus, when it comes to SLAs in the cloud.

Alan Levine: Right, and when it comes to restitution, we need to understand, as Matt said, that they're never going to pay to make us whole what we can hope is that they will help to shoulder some of the burden. Invariably, the stock SLAs, especially from the loud-- the large cloud providers, simply won't do that. They're going to give you a minor credit. They're going to offer you, as Matt said, some extra time or hours for the service that just failed. Oh great, give me another punch in the head. I love that. If you can negotiate anything in an SLA with a provider in terms of damages-- in other words, yes that e-commerce site went down. It was managed by this third party on our behalf, and so I've lost, I don't know, a million dollars over time in terms of e-commerce revenue, and you can build into the SLA that the provider of the service will help to shoulder some of that loss, some of that burden. In terms of writing a check, not in terms of offering you some extra service, offering you some free time, but actually helping to fill the financial bucket that has just emptied because of the debt of the outage that's the ideal situation, I would recommend that you don't hold your breath to receive it from the major cloud provider.

Matt Butkovic: Yeah, it's a great point, and at a at an individual level, if you're the CIO and CISO, kind of the worst time to figure this out is after something bad has happened. So, you know, for the good of your organization and the good of yourself and the good of your career, ask these questions up front. Understand your SLAs before they're at need, right? That's really what we're saying.

Alan Levine: Yeah absolutely, yeah. I mean, understand via your negotiations with your third party or service provider, what are the worst things that could happen? And then document the response in terms of what you will do, and most importantly, what the service provider will be expected to do in the SLA. That is part of the agreement now, and so once it's signed off, as I said in the beginning, that becomes a contractual relationship. They, the service provider, has committed to do x if something goes bump in the night. Understand exactly what it means for something to go bump in the night and then negotiate as well as you can to get as much of that x as you can if something goes wrong.

Matt Butkovic: Yeah. It incents behavior. At the end of the day, SLAs should incent behavior. Now, to be fair about all this before our Amazon prime is cancelled and our Gmail accounts are terminated, you have to be a good consumer in the sense too, that you're willing to do this in a manner that demonstrates good faith, right? What do I mean by that? I mean that there is a certain flow and life cycle to these relationships, just like any human relationship. So I believe this starts-- and this slide depicts the basic flow. It starts with a mutual understanding of those for security requirements, right? So at a very basic level, I can write down what's expected and the other side says, "I understand that. I can meet them,"

right? Once you've actioned that and have a few miles or kilometers or whatever distance interval you might use, of experience you can then develop what I describe as justified confidence. This partner, using the SLAs, has demonstrated that they are meeting the performance expectation, they're meeting the SLA, right? That's the next stage in evolution and not everyone gets past this stage, right? Well frankly, some never get past the first stage, but the third stage is really a trust, and I don't mean trust in some sort of cliched or trite way. What I mean is, you have high confidence your service provider will do the right thing proactively when there's any doubt about the decision we made. So instead of reverting only to the SLA and seeing that as a floor rather than the ceiling, they will flex and pivot if there's some extraordinary circumstance. That's real trust, that's real partnership.

Alan Levine: Right. I mean we talk about providers doing the right thing and, you know, one definition of the right thing is what anyone will do when no one's looking. And so if we go back to this notion that you may have constrained or restricted visibility into what the provider is doing, you may receive limited information in terms of their adherence to metrics, reporting, all the things that we've talked about. How do you get to that level of trust? And some would say, that comes from experience, you know, fool me once shame on you, fool me twice shame on me. I get that, right? Some of us can't afford to be fooled once though. One failure might be more than we could ever tolerate, depending upon what we have moved to a service. And so I think you need to build up as much confidence in advance. How do you do that? Talk to other customers of that service. Benchmark as much as you can. Understand what they move to the provider, what their expectations were, if you can. They may or may not agree to this. Take a look at their SLA. What were they able to negotiate? Sometimes those are secret, sometimes they're available. Wherever they're available, I would try and get your hands on it so that you can review all of the information you might need not to get to this nirvana of trust, but at least to move toward it, to be able to improve your level of confidence in the service provider. That's first, and so then level of trust in the service level agreement itself.

Matt Butkovic: Yeah absolutely, Alan. And we should also point out that this is bi-directional, which is, if you're a service consumer that's determined to needle the service provider over every little issue, you should expect that achieving that trust is going to be very difficult.

Alan Levine: Yeah, yeah, and I do believe it's bi-directional, also in the sense that, you know, where a provider can be flexible, can offer flexibility in terms of their service offerings, for example, their levels of cyber security defense or operations of visibility, or reporting, that's only going to be as good as you as the consuming organization know to ask for it.

Matt Butkovic: Right.

Alan Levine: And if you don't ask for it, in some cases you simply won't get it. The reason for that is, as I said earlier, some of what you asked for might have a price, and the provider might say "Well, I can give you what you're asking for, but I have to charge you for that." You might find that reasonable or unreasonable. It's a separate discussion. But if you never asked for it, well then, it's possible at least that you're not going to get it.

Matt Butkovic: Yeah. You'll never achieve that.

Alan Levine: So let me just say one other thing, because while we were talking, my Azure account was killed, my Google account, Gmail. In fact, I think I'm using an abacus once we get off the phone. Let me just say that, you know, it is in the provider's best interests to do things well.

Matt Butkovic: Yes.

Alan Levine: Especially cybersecurity. You know, Microsoft had that issue with Exchange recently. That was not a good headline, it was not a good hair day, especially for the security folks at Microsoft. They don't want those kinds of days. Oracle doesn't want those kind of kinds of days. AWS doesn't want those kinds of days. They want to be able to provide a secure and seamlessly interwoven service, interwoven with their customers' needs, right? And so certainly there are good reasons why service providers exist. In this day and age we couldn't exist without them and it is imperative simply that we as the consuming organization know what we're getting into before we sign on the dotted line.

Matt Butkovic: Thanks Alan, and I think what you're saying is really one of the key takeaways, right? And I'll leave the audience with this, right. I think you can divide these relationships into two phases. There's forming a relationship, and then ongoing management of the relationship, and each of these have pieces, parts. It's really underpinned by this iterative loop of SLAs, and your SLAs will change over time. Something we should also describe is that SLAs aren't sort of monolithic and never changing, right? They have to be able to change with your expectations for cybersecurity, the specific services you're subscribing to, and then the posture of the service provider. So with that, Alan, I know we're just about out of time and one of the things I worry about with the presentation like this, is this can seem really daunting for folks. I would argue, you can start small, right? But what I mean by that is, if you can take the time to chart out your most critical assets and your current expectations for securing and protecting those assets, that is the basic building blocks of the SLAs you need. So maybe in closing, Alan, what are some tips you'd offer the audience when it comes to SLAs?

Alan Levine: Yeah, so you have the word up on the screen. Let me emphasize it: relationship matters, and so develop a relationship with your service providers. Don't see them as some kind of just dark hole,

you know, the Wizard of Oz behind the curtain, that is simply providing the service. Develop a relationship, know the people. You might say, "Well, the people don't really run the-- or don't really offer the service. It's the organization." But yeah, organizations are made up of people, and so, you know, maybe they will go the extra foot, if not the yard, because you have extended the olive branch to build the relationship. I think that's number one. Number two, as I said earlier, don't develop an agreement without your procurement and legal folks right in the middle of it, because that is a commitment which is a contract, and no contract should ever be signed by an organization without procurement and legal in the middle of it. And then third, and you kind of said this a moment ago, Matt, know exactly what you're asking for, right?

Matt Butkovic: Right.

Alan Levine: Because invariably, if you don't know what you're asking for, the one thing you can be sure of is that you're not going to get it.

Matt Butkovic: Exactly right. Yeah. Well, Alan, I really appreciate your time today. I know you and I feel strongly that this is a key subject for all cybersecurity practitioners. If folks are interested the SEI, and specifically the CERT artifact catalog, has lots of guidance about third-party relationships. We do interesting research there, so please do please do have a visit to our website if you're interested. So Shane, back to you.

Shane McGraw: Matt and Alan, great discussion today. We really appreciate you sharing your expertise and just a just a great conversation. We also would like to thank each and every one of you for attending today. Upon exiting please hit the like button below, and you can subscribe to the SEI YouTube channel by clicking on the SEI seal in their lower right corner of that video window. Lastly, join us for our next livestream which will be tomorrow May 12th, and our topic will be, how do we teach cyber security? by Rotem Guttman. Registration information is available on our website now, and it's also in the chat. Any questions from today please send to info@sei.cmu.edu. Thanks everyone, have a great day.

Matt Butkovic: Thank you.