Risks, Threats, and Vulnerabilities in Moving to the Cloud

featuring Don Faatz and Tim Morrow as interviewed by Eileen Wrubel

---

Eileen Wrubel: Welcome to the SEI Podcast Series, a production of the Carnegie Mellon University Software Engineering Institute. The SEI is a federally funded research and development center sponsored by the Department of Defense and operated at Carnegie Mellon. A transcript of today's podcast will be available at sei.cmu.edu/podcasts.

My name is Eileen Wrubel, and I am the initiative lead for the Agile in Government practice here at the SEI. Joining me today are Don Faatz and Tim Morrow, both of whom are researchers here at the SEI. Today, they are joining us to talk about risks, threats, and vulnerabilities in cloud computing. This is the first of a two-part podcast focused on their work in cloud computing.

Welcome, Don and Tim.

Don Faatz: Hi, Eileen. Thank you, it's good to be here.

Tim Morrow: Yes, thank you very much, Eileen.

Eileen: I would like to start by having you both tell me a little bit about your backgrounds, your work here at Carnegie Mellon, and the work that you did before you arrived here.

Don: Just prior to coming to Carnegie Mellon, I was at the National Cybersecurity Center of Excellence developing security solutions for industrial control systems used by electric utilities. Since then, I have focused on cloud computing security. I first got involved in cloud security a long time ago, at least in cloud terms, back in 2009, doing a quick-look assessment for the Intelligence Science Board to see if there really were security issues, which has actually led to years of understanding those issues.

Eileen: Okay, great. And Tim?

Tim: I have been here 15 years, so it is hard to remember back before that, but I did a lot of work with the Navy and dealing with nuclear reactors and things like instrumentation control. I have done mostly hardware, software type of background.

Since I've been in the SEI, I focus on architecture areas and the full lifecycle, trying to figure out how we can get our stuff into systems as quickly as possible, so it has provided a great platform to do that.

Eileen: Great, thank you. Today we are here to talk about cloud computing, specifically risks, threats, and vulnerabilities. Can you begin by telling me about the current state of the cloud and why you thought it was important to explore this right now?

Don: A lot of organizations are beginning to see the value of using cloud-computing services. But, for the most part, they end up with a hybrid form of IT environment, since not everything can just pick up and move somewhere else. So you will end up with some of your IT in a cloud, some of it on-prem, which creates challenges for figuring out exactly how to secure that. So we went down a path of trying to help with that. If you look at large organizations like the DoD, they have embraced this. They are looking to buy infrastructure as a service and even moving office automation to the cloud. For smaller organizations, though, it is something of a challenge, so we wanted to look at and give people some ideas about the challenges they will face when they do this.

Tim: From our perspective, working with our customers, a lot of times we work with federal agencies and they have the Cloud First Directive, which came out in 2011, to identify that before you go off to procure any type of computing center or device, you have to first consider cloud. But we have seen that there was not a lot of guidance for organizations to follow in that manner.

So a lot of times they went ahead and just did that; they would put stuff in the cloud and now they are sorry because they have had problems with that. A lot of the misconception was dealing with the understanding of a shared responsibility between an organization and the cloud service provider. Most people would say, *I just put it in the cloud, and it's secure, it's not my responsibility*. So that is part of what got us started in this area.

Eileen: Now let's move on and talk about those risks, threats, and vulnerabilities. I understand that you two outlined a number of commercial, financial, technical, and other kinds of risks, threats, and vulnerabilities in a recent blog post. Can you tell me about those and how you went about identifying them?

Don: We put together a collection of something called mission threads, where we look at how someone will use things, and then we look at what bad things might happen. We identified a collection of risks and threats and vulnerabilities. Some of them are unique to the cloud environment due to the characteristics of cloud, and some of them are things that you would encounter in on-prem IT also, but your ability to address them may be different in the on-prem case.

We are going to talk first about the cloud-unique issues, the first being that you lose some visibility into the infrastructure and what's going on when you hand over things to the cloud service provider. The service provider ends up having a shared responsibility, as Tim said, to have visibility into the portion of the world that they operate and are responsible for. This is a big change for most organizations that are used to complete visibility from the hardware all the way up through the application. So there is some adjustment in dealing with that.

The second area is that cloud provides on-demand self service, it's one of the five fundamental characteristics of cloud computing. It means that it is much faster to get access to resources than if you had to buy them and install them. The downside of that *much faster* is that anyone with a credit card and a keyboard can basically go and acquire resources, so you end up with what is often referred to as shadow IT in your organization, where people are using cloud resources and you don't even know about it, and so you have no idea what your risk exposure is from these resources.

Another one of the fundamental characteristics of cloud computing is broad network access, meaning you can get to it from anywhere. The other things you can get to from anywhere are the management interfaces that your privileged users use to construct and manage your virtual infrastructure. In your on-prem stuff, that's all in your network and not accessible from the outside. So in this case, you have to take into account that those APIs have to be accessible over the internet for everyone, and so you have some exposure there that you are going to need to manage.

The next one is separating tenants. The whole idea behind cloud computing is you share infrastructure with other people. That way you don't waste infrastructure resources, and your costs go down. So you may be running on a machine with half a dozen other customers, and there has always been a concern that, *Oh, what if my stuff leaks to them or their stuff leaks to me*? Historically, I think Tim and I would have told you, *Oh, this is not a big deal, the cloud service providers have done a great job, and life is good*. Then earlier this year the Spectre and Meltdown hardware vulnerabilities were announced that basically allow at the hardware level for something like that to happen.

Collectively, I think our opinion is still that you are better off using a major cloud service provider. Because if you think of people like Microsoft, Amazon, Google, they have enormous resources, and they understand the hardware much better than most organizations. And they have the ability to do something about it. If you are faced with, as everyone is, having hardware with this vulnerability in your data center, what are you going to do about it? You are going to wait for your vendor to do something, whereas the cloud service providers can respond quickly. So, while the level of concern here may have gone up, we still believe the cloud service providers are in an excellent position to deal with the problem.

The last cloud-unique challenge is that when you delete data, it might not actually be gone. If you look at a typical web application deployment into a cloud, you will find out that data moves all over the place. It may start out in the web server. If you use a content-distribution network it may go there. If you do backups it may get snapshotted into the backups. If you archive the backups it gets moved there. Each of these things is a unique and different service, and each of those services may have different data-deletion capabilities, data-retention policies, so you really have to look across that and understand what is going on. You also have to try and understand what your service provider does with media when they are done with it: do they sanitize it, do they destroy it? You need to take these things into consideration when you are deploying something to a cloud service. So, Tim?

Tim: I got to do the part here that is both on premise and cloud specific. A lot of times people are familiar with credentials being stolen, but it makes a huge difference when you are going into the cloud, and you have that occurring. Not just with your own service—like you as an organization when you start to use cloud access, you are going to have somebody responsible for allocating those services. If somebody would obtain their credentials, then they could be setting up all kinds of VMs, doing a lot of things, or impacting what you already have out there.

The other concern in this one is the credentials associated with the cloud service provider, because they are not just doing one organization, they're doing many. So that's a very critical aspect that people need to consider about that.

Another area is when dealing with vendor lock-in for cloud services. You can hear about cloud service providers and the functions that they do, the services, and they sound pretty similar, but when you go to implement them, they are unique. It is a concern that you need to realize that to put your data in there and to use it, say, like in a software-as-a-service model, you have to realize that when you go in there that your stuff is going to be tailored, they're going to tailor it to how they maintain their system. And if I'm interested in pulling that out, it's going to cost me time and effort.

The other thing that people think about with lock-in is concerning, when you put your information into the cloud, it's very easy and quick, they have a lot of methods to do that, that's low cost. But to take it out, they charge you more for that, and the methods are not as convenient. So when you hear people saying, *Oh, Amazon's got a sale this week, maybe I should switch from Azure*, you can't do it that easily. So that is the concern in that area. There are many things that you need to think about once you put your stuff up into the cloud, to be able to take it away.

The third one that I was going to talk about was increased complexity strains your IT staff. So when we were working on our papers, we would run into organizations that are smaller; different government or DoD organizations that have small IT staffs. Now you are asking them to not only

do their on-premise, which they are used to doing their normal data-center stuff, but then you want them to understand what it takes to go up into the cloud and do that safely. The security is different for that aspect, and then each of the cloud providers, how they implement it is different. Now you are kind of doubling, tripling, if you are going to do a multi-cloud environment. It's going to take a lot more knowledge that will have an impact on your IT staff to be able to get them to effectively and safely implement these functions.

The fourth one I wanted to talk about was the supply-chain compromise for a cloud service provider. A lot of times with the government, there is very strict guidance for what you have to know and understand for you as a program to be able to say, *I feel real comfortable with this product being delivered by my vendors. I have to understand all the way down to the lowest subcontractor, who's doing what*. You don't get that in the cloud with the big cloud-service providers. That is something you as an organization need to worry about, *can you satisfy your own requirements?* You have to develop a relationship with your vendor to do that.

The last one, and you are going to hear more about this in our follow-up podcast, is insufficient due diligence. Like I mentioned earlier, in the directive to go cloud first, people jumped and they put their stuff up there because they want to say, *Yes, sir, I am going to be there*. But there is a lot to this, and that is what our papers expand upon. It is not just identifying the threats, but then you have to think about the full lifecycle and the impact from cost, personnel, staffing, training, all that stuff. There is a lot that you have to do. So it's not something that you take lightly, and that is a concern we want people to understand.

Eileen: So it is really easy to provision cloud services, but actually making sure that you are doing the organizational due diligence and preparing the work force is a whole other can of worms.

Tim: Absolutely, there's a lot to it.

Eileen: If someone in our audience wants to learn more about these risks and how to mitigate them, where should they start? What is out there for them?

Don: The first place to start is with the major cloud service providers like Amazon, Google, Microsoft. They all have trust and security webpages and a wealth of resources where you can read about all the different concerns, you can read about what those particular service providers are doing about it. You can learn what kinds of third-party assessments and certifications are there to help you understand the security of those services. Also, you need to keep track of what is happening in the world. *What threats are evolving? What bad things are happening that might be affecting cloud service providers?* So there's actually a wealth of free and public information there as well. Interop publishes a State of the Cloud report every year. Everyone is probably

familiar with the Verizon data-breach report that has been going on for a long time, and it now has some cloud incidents in it. You can see what happened there in those cases. Then, the last place, IBM now has an X-Force Threat Intelligence report, which also focuses on threats to cloud computing. So all these are open, available on the internet, and free to everyone. Tim?

Tim: And some of the areas that we found helpful, too, is as we've talked about these hybrid multi-cloud environments, there was a new category of companies coming into place, they're called cloud access security brokers, which they're marketing as a single pane of glass. So, rather than needing to know everything, you have somebody that comes in that says if you use my service, I can handle your identity, access management configuration, and help you with security. So that's a real good area because to understand the problems you face, that's what they're out there advertising that their product's about. So I would look at their different sites to learn about that.

I like podcasts, security and cloud podcasts: Security Now, Cloud Computing Weekly were ones that helped me a lot when we started doing our initial development work. Good websites, Cloud Security Alliance and ENISA [European Union Agency for Network and Information Security] page on cloud security], were two that were very good dealing with government and concerns that they have moving things to the cloud.

Eileen: What is next for both of you in this field? Are you working on any more collaborations?

Don: Yes, Tim and I are going to continue working together on security for hybrid and multi-cloud scenarios. We are preparing a report on best practices for securing that environment, which will look at what you should do to address the various risk sets and vulnerabilities that we talked about here.

Tim: We are also looking into that shared responsibility model and understanding that to help convey what an organization needs to worry about as they go to multiple cloud providers. I think we are starting to see, too, the big cloud providers are seeing that it is not okay for these security-access cloud brokers to take up their business, *I can bring in some of that work myself*. I think that shared responsibility model is starting to change. We are starting to see where they are bringing in some of this service for their own. Whereas in the past they have been more standoffish and let each customer deal with their own security. Now they are saying well, maybe I can help you with that. I think we are going to look into that because that has changed very recently; there are some new services that impact that.

Eileen: Great, I'll look forward to hearing more about that when you do that work. I would like to thank you both for joining me today to talk about this work, this is really interesting to me. I look forward to talking to you again soon.

Tim and Don recently co-authored a blog post outlining 12 Risks, Threats, and Vulnerabilities in Moving to the Cloud. You can read that blog post at insights.sei.cmu.edu. Click on the author tab and search under M-O-R-R-O-W. Also, please note that we will provide links to all of the resources mentioned during this podcast in our transcript. Join us next time when Tim and Don join me to talk about cloud security best practices.

This podcast is available on the SEI website at sei.cmu.edu/podcasts, Carnegie Mellon University's iTunes U site, the SEI's YouTube channel, and on SoundCloud. As always, please feel free to reach out to us with any questions at info@sei.cmu.edu. Thank you.