uberknowledge

# John Yeoh, VP of Research, Cloud Security Alliance

## Cloud Security is a Shared Responsibility

John talks about CSA's main areas of focus, the challenge of staying up to date in an ever-evolving space, and the importance of participating in new learning.

| | |
|---|---|
| 01:50 | CSA's three areas of focus are helping people transition to cloud, enhance cloud security,and adopt new technologies delivered through cloud. |
| 05:37 | Cloud security needs to be based on a shared model. |
| 10:52 | How you build security culture within your organization? |
| 15:00 | Education and training is a constant. Read, absorb, download, but most of all, participate. |

**Ashwin Krishnan:** [00:00:40] We have another guest at Black Hat, this is John Yeoh, who is the VP of Research at Cloud Security Alliance (CSA).

**John Yeoh:** [00:00:49] Ashwin, thanks for having me.

**Ashwin Krishnan:** [00:00:50] Absolutely. So, John, talk a little bit about CSA. I know CSA just celebrated 10 years, if I remember, right?

**John Yeoh:** [00:00:56] Can you believe it? Yeah, I think people thought we wouldn't last this long.

**Ashwin Krishnan:** [00:01:01] I really wanted to kind of probe a little bit. When CSA first started, I think cloud was probably still in its infancy.

**John Yeoh:** [00:01:08] Oh, yeah, absolutely.

**Ashwin Krishnan:** [00:01:09] So what was the calling point to create an alliance in the first place, and where are you today, and what is the path forward?

**John Yeoh:** [00:01:17] Yeah, the call for action back then was how do we really understand the right way to secure cloud computing? How do we develop trust? How do we provide evidence for that trust? How do we take advantage of what cloud had to do to maintain security? And it seemed like a typical third-party assessment. But it wasn't, right, because I think with a lot of third-party vendors, you're not relying on them as much as you do with cloud services where you're offloading and outsourcing a lot of what we do in-house. So that was definitely very different.

"How can we help people build new tools in the cloud and enhance their security posture even more?"

[00:01:50] And ten years later, I think we've talked about this internally, maybe we thought — just because of the concept of cloud — we thought maybe we'd be a little bit farther than we are today. But with that said, I think we've done a lot of amazing things. We understand cloud a lot better. The three areas I think we try to focus on, we're still continuing to help people transition to the cloud. And I think that's important. We're still seeing organizations that are new building cloud strategies and want to do things like that.

[00:02:15] The second piece is, we have a lot of people now that are in the cloud and they've met the general requirements that are usually imposed on them by their regulators — whatever industry they're in — but how can they enhance security better. There's a lot of good cloud tools, methodologies. DevOps is one of them. So how can we help people build new tools in the cloud and enhance their security posture even more?

[00:02:41] The third element is those that are very forward-thinking and looking to adopting new emerging technologies like IoT, blockchain, and all these are going to be very managed, orchestrated, and fulfilled through cloud computing. So that's an element that we want to focus on. Those are the three areas, I think that as organizations mature, as our member organizations mature, that we're able to take them through that entire journey.

**Ashwin Krishnan:** [00:03:03] Excellent, so let's talk about number one and number two. I think there's this whole digital transformation or journey to the cloud. That gets attention, budget, and you get these projects that are fun.

**John Yeoh:** [00:03:16] Sure.

**Ashwin Krishnan:** [00:03:17] The second piece, and I've had this debate on Twitter with an interesting group of people, and they are CIOs and CISOs combined, is once you're in the cloud ... Taking Capital One as an example, not so much about their breach per se, but when they decided to do away with the data centers and move to the cloud. There's a mental shift that needs to happen because you're no longer in. You're not the same. You don't worry about power. You don't worry about cooling. You don't worry. You should technically be thinking about that cloud as much as you would have your personal data center, which you can see and feel and touch.

[00:03:51] Mentally, how do you not outsource responsibility, not outsource the cognition of the data center is still yours, the data is still yours, and it's being run by somebody else? What do you think in your member community? What is phase two, does it really lead to complacency?

**John Yeoh:** [00:04:13] Well, I think changing mindset is probably the biggest bear on anything. Is it psychological? Is it real? If you've been in security a long time, if you've run your own infrastructure for a long time, what a difference it is to now try to outsource this and offload it. So that's the one we're talking about, where people who are transitioning to the cloud, it's still a challenge for them because they have this mindset of, I still want to own this. I still can't test this in a cloud environment. So, it's different.

"We're seeing the security bar raised with a lot of cloud providers."

[00:04:43] Then you have the other people, the new people, who are like, "This cloud is amazing. I can just outsource everything and just offload all my security onto my provider. This is great!" So, you have two scenarios. And I think it's good, too. We're seeing the security bar raised with a lot of cloud providers. In fact, we've even seen this too, in our latest top threats report. We do a top threats cloud report every couple of years. And this year we actually saw that a lot of threats that we saw rise to the top were actually further up in the technology stack. So, things like system vulnerabilities, shared technology vulnerabilities weren't as high on the list anymore, which to me maybe gave us a perception that people are more comfortable with cloud, especially the foundation of cloud services and security there. They're more concerned about things that popped up that were new misconfigurations and architectures and cloud environments.

[00:05:37] So I think we're seeing some of that kind of flip, what can I take ownership of better, what do I have ownership of, and what can I do about that? It's not just an end-user thing. It's not just the customer side. I think the providers need to also allow safe and secure default configurations. I think we're going to see notifications on if I have something exposed, an exposed cloud instance, maybe it has access to too much of my cloud storage, there's some bells that are ringing off so that I'm aware of

that. So, yeah, I think those are the challenges that we continue to face. It is a mindset of, I can rely on my cloud services for some of that security. And then the new people think, even though the cloud provider is taking care of some of my security, what do I have control over, what do I still need to be responsible for? And that's always a challenge, I think, across all our members to really understanding that shared response to be modeled not just with the providers and themselves, but even across their own organizations. Because now it's saying that all the units that are on cloud services, they also need to be to understanding security, not just the security teams. Everything is not filtered through the security teams anymore, so shared responsibility, provider and user, even in and across the end-user's customer base.

**Ashwin Krishnan:** [00:07:08] That's a great segue into my next question. A comment you had posted on LinkedIn on Brian Krebs' article on the Capital One breach, where you said "specialized knowledge of cloud platforms is such a need. Stay up to date ... if you can." So TMI is plaguing, in fact, I remember last Black Hat a few people were saying coming to Black Hat puts them back about a month of just keeping up with stuff.

**John Yeoh:** [00:07:29] The "if you can," it's kind of funny.

**Ashwin Krishnan:** [00:07:33] I mean, how does somebody even keep up with one cloud, let alone multicloud?

**John Yeoh:** [00:07:39] I remember going, eight, nine years ago, playing around the cloud platforms and they'd add 26 features, "Oh my gosh. I got to keep up with those! What are these?" It's so hard to do. We're seeing some of the major platforms add 1,800 features this year to their cloud service, which is fantastic. Wow, that's incredible, but how do you possibly keep up with that? How do I know what features pertain to me? Do I understand if they're turned on or turned off? Do I understand the configurations of if I'm doing something the same way it was the whole time, but now is it different? And those are the things where I think your organization needs to have an expert on the cloud platforms and services you're using. That's a must read because that's where we're seeing most of the errors are not knowing how to utilize these services, set up these services, configure them properly. But the challenge is, how do you do that? They're so progressive. I think functions and features are fantastic, but how do we possibly educate the consumer on those? How do you keep up with that? How do you tailor that specifically to their need? That's the biggest challenge we have in cloud.

"Most of the errors are not knowing how to utilize these services, set up these services, configure them properly."

**Ashwin Krishnan:** [00:08:46] Has there been any talk of that at Black Hat at all? Like you said, it's one thing to have 1,800 features and another thing to know how secure are those 1,800 features and which ones apply to you.

**John Yeoh:** [00:08:57] Within the CSA, we try to be very agnostic when it comes to

cloud services. So, all our training and education is very baseline, standard cloud security. This is how you would build this new infrastructure. How would you implement that? Depends on the services that you're using. But we've partnered with a lot of providers on doing security roadshows around the country with specific regions. We'll leverage the CSA audience. We have over 400 different companies that are part of us now. We'll invite them to these roadshows that we do with different providers, so they can learn a little bit more about the services, how to set them up. But again, we can't go through 1,800 features.

**Ashwin Krishnan:** [00:09:38] You can't either.

**John Yeoh:** [00:09:38] [Laughs] I've talked to even major cloud engineers with these major platforms who can't keep up with the features and functions.

**Ashwin Krishnan:** [00:09:46] So it's a problem that we don't have any near-term solutions to?

**John Yeoh:** [00:09:49] Yeah, we don't have a near-term solution, it's just understanding how it's set up and hopefully that will help.

**Ashwin Krishnan:** [00:09:58] So going back to something you mentioned earlier, the tension between the security group and a line of business. The security group locks down saying, "You can't use your favorite AWS/Azure feature because we haven't tested it, we haven't figured out what the baseline security configuration is." And you have lines of business saying, "I want to use the latest and greatest because my competition is killing me." So, going back to cloud, is it creating this chasm inside organizations, where you have developers who are now saying I want it all, and unless you have a security-first mentality — which is maybe starting to change, having some discussions around that — then you're essentially back to the "No" group.

**John Yeoh:** [00:10:52] Boy, same old story, right? It's the mom and dad just scolding the child: Are you doing your security? Are you brushing your teeth? I think that's something that's always a challenge. How do we build that security culture within your organization? We try to outline steps for organizations, especially, you know, we talked about DevOps people because that's what we want to do, right? When we have a job to do, we want to do it fast and quick and easy as possible.

"Can you really stop your business units from utilizing cloud services?"

[00:11:22] So can you really stop your business units from utilizing cloud services? Certainly, there's some, maybe federal agencies that have a little more strict requirements around that. But for the most part, we're seeing organizations can't. That's why Shadow IT has been a common term that we've been using in the industry for the last few years because cloud services are being used that you're unaware of. **So, is there a way that we can enforce security policies on tools that we're not aware of**? We're able to do that a little bit today, which is really good, but **it's best to build that security culture**. How do we do it? We talked about responsibility not just being for the provider, but across your organization. You know, we talk about providers are they educating me on their services; are you educating your staff on security? I think

that's very important. And hopefully, CSA will play a role in that with a lot of organization that we're working with. But I think it's important, security culture. How do you do that? And once you have that, you can align your business needs, you can build tools successfully. Easier said than done, but it's a challenge that we all face.

**Ashwin Krishnan:** [00:12:26] So talking about your membership, you've mentioned about 400 members. Are you also seeing the composition of the people who attend CSA seminars or go to CSA conferences, not just be the security group? Are you seeing a bigger spectrum of stakeholders joining CSA?

**John Yeoh:** [00:12:45] Yeah, and in a few different ways here. The first way we're seeing is when these companies join CSA. In the past, it's been a lot of cloud providers wanting to get the message out, share what they're doing in the community, what kind of services they offer. But almost half of our members now are large enterprises, end-users that want to understand how to navigate through this complex cloud landscape. They want to understand how people are leveraging tools. And I think that's really important to just talk about these things. Let's not be quiet anymore about security, about breaches. Let's talk, let's share, let's learn what went right, what went wrong. And we're seeing more of that too, in our events, in our forums, where it's not just the security people, it's the compliance people because now what's being imposed on us, regulations. New privacy regulations are being imposed. So now we have privacy people that are interested, and then we have the technicians and even the developers too because we talk about that cloud tooling that's so exciting and the DevOps methodology, the DevOps movement about empowering dev and building security that way. So, we have organizations that are moving their developers to learn more about security and make sure that they have that security-first mentality. So yeah, we're seeing more stakeholders from the enterprise side, from the end user. We're seeing a much broader scope of participants, too. Like I said, not just the security teams, the compliance people, the developers because we all have a stake in security. It's nice to see that; it's nice to see that diversity.

"Let's not be quiet anymore about security, about breaches. Let's talk, let's share, let's learn."

**Ashwin Krishnan:** [00:14:23] That's good because, like you said, it shows that there's a greater interest in security. Switching gears to certifications, for many, many years having a CISSP, that was your claim to fame, right? You were certified and you could go anywhere.

**John Yeoh:** [00:14:42] Yeah. It's still great to have.

**Ashwin Krishnan:** [00:14:46] Cloud, as we talked about, it's fast moving. So even if I were to get a cloud certification today, it could be redundant in a week from now, if I haven't kept up. How do you deal with that?

**John Yeoh:** [00:15:00] Well, you're right. Education, training, it's a constant thing for us, especially in this industry that's so dynamic. We see so many changes. Within CSA alone, we have a cloud certification, too. It's called the CCSK and we're on our fourth

version of that. But even within versions, we have a new LMS system where you can actually go online and learn about the major domains and the major structures and how we build out that program. But on top of that too, we're adding emerging technologies — what's the latest in research, what else can you learn about — because it's a constant thing. We offer webinars free, not just to our members, but it's open to the public, too. So, I think that's a constant thing. CSA, we're an education tool. We're a platform. I think it's not just about absorbing but participating. I think that's where the key is too. So all these education tools, these webinars, these guidelines that I talk about, they're fantastic. They're snapshots of what really happens. The strength about CSA, about education is participating. We can go back to, you know, professors saying, you're going to get out what you put into this class. And that's life, that's security, that's cloud. And CSA is one of those engines, one of those platforms where you can actually participate. And I tell you, our guidelines, our research takes sometimes 300 days to develop something like that. So you can imagine the man hours, the contentious discussions, the back and forth of this is how we did it, this is how I did it, coming up with a pattern that reflects the best practices, the best known methods; we share that to the community, which is great. Read it, absorb it, download it, but participate, be a part of it; I think that's where the real education is.

**Ashwin Krishnan:** [00:16:46] One final question. We are at the end of the Black Hat week, the beginning of DefCon. What were two things, one positive takeaway that you found uplifting and one which you maybe didn't expect, but you're bummed to have seen it.

"Read it, absorb it, download it, but participate, be a part of it; I think that's where the real education is."

**John Yeoh:** [00:17:16] You know, I think one thing that was kind of a surprising takeaway was we had a large breach that happened last week, the Capital One breach, and we saw it broken down a little bit more, what happened there. The AWS platform wasn't penetrated. It was misconfiguration error on the customer side, too much access, things like that. I think one of the things that was pretty exciting about that … I shouldn't say exciting because that's kind of a bummer, too, right? Breaches are never fun when over 100 million accounts are exposed. That can be my bummer.

[00:17:56] But one thing, if we think about what Capital One did with AWS to not only speed up the investigation of what happened — we uncovered this in less than four months, you know, we discovered the breach. And within 10 days, less than two weeks, they are able to provide evidence through cloud tooling, through AWS's logging information, find out the IP address, track down the suspect, and come to an arrest. Let's think about that for a second. I mean, if you've been in this organization for a long time, we've seen APTs that can just live around for years. Tracking someone down, building an investigation, and arresting somebody within under two weeks, that's remarkable. And that's incredible visibility that we have today. That's incredible tooling that we have today. And that was the real thing that I walked away with, even though, yes, there was a breach, and that's never a good thing when we lose customer information, but how we responded was incredible: incredibly fast,

incredibly diligent.

**Ashwin Krishnan:** [00:18:56] That's actually really important because sometimes we get caught up with the negative side of things, which is obviously bad. But the flip side, being able to detect, identify, and get the person.

[00:19:10] This is great, thanks for your time, John. Hope you have fun at the rest of the conference.

**John Yeoh:** [00:19:17] Definitely, Ashwin. I need some fresh shoes and a tall glass of water. It's been a long week.

**Ashwin Krishnan:** [00:19:23] [Laughs] Thanks, John.