# Jim Reavis, CEO and Co-Founder of Cloud Security Alliance

## Communities, GDPR Opportunities, and Security in IoT

Jim advocates for greater transparency within the security community, points out that GDPR means privacy must be the differentiator, and addresses the challenges of security in IoT.

03:17 Vendors need to information share.
07:36 You don't need to give away your secret sauce to be part of the community
12:47 The trend for communities within communities
13:38 Trust and transparency still requires face-to-face contact
15:42 GDPR actually creates opportunity
19:28 The challenge of security in IoT

Ashwin Krishnan: [00:00:01] So, welcome to Black Hat. With me is the CEO and co-founder of Cloud Security Alliance (CSA), Jim Reavis. We were talking, just before we engaged in the dialogue, about one of the big challenges right now — just given the number of cybersecurity companies out on the show floor today — is the problem that they're trying to solve versus the true problems that practitioners and CISOs are really trying to solve. So, from your vantage point, where you actually connect with both communities on a regular basis, what do you see? Is there a divide; is there friction; are the vendors doing the right thing? Could they be doing better? Are the CISOs not communicating enough?

Jim Reavis: [00:00:50] Thanks for having me on your podcast. Yes, I do think we have a divide that is a product of different constituencies having different goals, different initiatives, and there's not necessarily a right or wrong there. But it's a very complex community that we have, in that it sort of arose in a very informal manner, the way information security even happens. We've had people who in their day job may even be a legitimate member of the industry, but at night they are criminals. So, it's very interesting how it's come about. The issues of how the vendor community can solve the pain points appropriately of the end users is a real challenge.

I was asked, maybe 15 to 16 years ago, by a vendor to give some perspective of the end users to the sales team, so they could more effectively sell to the CISO. So I said, "OK, I'll do that." But how I did that was, I went to one of the biggest companies, to their CISO in the US, and said, "I want to do a day-in-the-life. Give me your calendar. Let me look at it and then let's go present that and break it down." This person is from a global company. They are scheduled from 5:00 a.m. to 8:00 p.m., there's literally bathroom breaks put in there, they're so busy they're trying to do a lot with a little and the numerous vendor pitches are getting hard to do. So, there is a lot of leaning on maybe a few different systems integrators, and built relationships that can help aggregate some of the different solutions that are out there to help them. Big, big challenges.

You know, I think that it's the nature of security, where we don't share, and enterprises don't share with each other. A lot of times they really want to share. CISOs have quit their jobs in frustration because they have detected malware or threats that they felt would be very important to let their competitors, or even companies and competitors — like a local CISO community, know about and maybe their legal prevented them from doing that. So, there's definitely a lack of transparency and ability to share that happens from the customer side. Here's my real problem in a very streamlined manner. Certainly, they get you in there under an NDA and it’s the same for the vendor side; it's capitalism, it's the free market. We're competing against other companies who have the best cloud security solution, the best CASB, whatever. Ours is best, everybody else's is a piece of dog do, and we want to make it as hard as possible for you to use any other solution. Then the threat vector is just constantly changing. You get to this whole, “Can we go with one company and have them do a lot of things, or do we have to do this best of breed and match a lot of different areas?” I think the world of cloud, the public cloud — social media actually helps a lot of this too — is more transparency around publishing threats and vulnerabilities and best practices and really how applications need to get mashed up together with publicly-known APIs. It's driving a little better and more towards that. You're starting to see some government requirements of disclosures and things like that. So, it was built foundationally not to be functional, it was built to be dysfunctional in terms of how this is happening. I think we're just brute force and getting better with how technology is being consumerized. So, we'll see where that goes.

Ashwin Krishnan: [00:05:43] Wow. So, we have enough to chew on for the next 20 minutes or so. Let's start with something that truly resonated with me. Having come from the vendor side, I never thought of it that way — and I'm pretty sure I'm a proxy for all of the vendor community out there — a day in the life of a CISO, a day in the life of the VP of Security Operations and looking at his or her calendar and thinking what can they stop doing in order to hear my pitch? That recognition, the empathy with the buyer side versus constantly bombarding them with e-mail pitches and calls, that's number one.

The second thing that you talked about, this comes back to the CSA and your role, is how do you provide a fabric for more open sharing among the CISO community, and even among the vendor community, without revealing your roadmap or strategy? My personal view of this is part of the reason why vendors are doing what they're doing, in terms of out noising each other out, is because they don't hear the other competitors actually pitching to a customer. In my life, if I heard six or seven of my competitors pitch the way I'm pitching to the end user, I'd say look this isn't working. So, given your position on what CSA stands for, is there a bridge that could be formed where there are these groups saying, "Share what you are seeing so that we can all come out ahead"? Otherwise you're going to be on the show floor listening to essentially dazed people walking aisle after aisle and probably not understanding what each vendor does.

Jim Reavis: [00:07:36] Right. I think it is about inclusive communities and finding common interests that everybody can agree on. I'll give you an example of what we do there. It's important for companies to understand, the secret sauce of what you do doesn't need to be part of the community. But a lot of companies think everything they do is with secret sauce and that's the issue. That's where standards really come in. So, a really good example is the CSA STAR program. The STAR program is something that we started in 2011. It was based on something we built in 2010 called our top controls framework, which is a very high-level set of control objectives. The idea that we had in 2011 was, "OK, we've got this questionnaire that's a standard one, and instead of just having every end user go send the same questionnaire to every vendor, let's create a registry of these." And shout out to my friend, Becky Swain, she came up with — we had some very bad acronyms — she put Security Trust Assurance Registry: STAR. So, the idea there is let's create transparency; let's let all of the vendors put their best foot forward in a very public way and say, “Here's how we address the cloud controls matrix. Here's our security controls.” On the enterprise side, because they're not doing things right, every enterprise has historically had their own vendor-procurement security-assessment posture which is unique, and it's a win-win for both sides because they all came together to build the questionnaire. Everybody put what was in there, and is it 100% perfectly aligned with every company's unique needs? No, but it's 90%. So, it's an example of where we can reduce a million different unique questionnaires that every company needs to go deal with and that that adds up to a lot of time in the compliance calendar on the day in the life of the CISO, security manager, compliance manager.

It's one example and the barriers for that are on the vendor side. It's like, "Oh, we don't want to show too much of the kimono, we're worried that someone might look and criticize, our competitors will criticize how we answered it." Well tough, you need to go out there and just do a better job of securing your solutions or explain how they work. And on the end-user side, it's like, you can't have this “not invented here” attitude. You need to just say, "I've built a great questionnaire, but I'll use this industry standard one and if there's anything that comes out of that, maybe secondarily, where I need to go address additional risks I am concerned about, I can do that," and that's much more streamlined. So, that's an example. But that's what communities — and that's very important in information security because it's always been, I call it the old private fire brigade, "I'll protect my building and the building next door will burn down." — when you're in a community and you build those face-to-face relationships and you agree on standards, you help each other. We all help each other and that's what we're trying to do.

Ashwin Krishnan: [00:11:05] It's interesting you mentioned the word community because when I think about security and community, the first community that comes into my head is the hacker community. The provocateurs, the miscreants have a pretty tight network. They work together to solve their problems. The initiative we talked about is a really important one, but at what level do vendors need to start realizing that card swiping at trade shows and how many people stopped by your booth is no longer the measure of your success? Is there a cultural transformation that needs to happen to these organizations? I'm the VP of Marketing, I come to Black Hat and tell my boss, "I had ten card swipes, but I had these twenty great conversations with customers about solving real-life problems," versus saying, "I need to have 2,000 card swipes otherwise our ROI isn't there." Are you seeing that the vendors are starting to hold themselves to a higher bar because otherwise it's the first thing that you get from your boss when you go back to your cubby hole?

Jim Reavis: [00:12:19] Yeah, it's funny that you'll see, for example, a company that is promoting itself as a great GDPR solution or consultant, yet it breaks every single GDPR guidance on its website to try to generate leads. I mean, we're bipolar. It's just crazy how we think about this, and the drive to compete is very hard. We're starting to really understand that and, yes definitely, I see this trend towards communities within communities, maybe smaller events, maybe special birds-of-a-feather dinners, or other online groups or things like that, that the Black Hats and the RSAs of the world fit in, but they only have a certain purpose here and it's very hard to have substantive types of conversations here. So yeah, there's still the mentality of let's get a big bucket of leads out of this, we're going to measure that, but they are starting to think in multiple dimensions, and then let's also have some of these more focused conversations. I think that the challenge, and it's not just for security but security needs to be a leader here, is understanding protecting privacy of people who are part of your marketing program, collecting as little information as possible. That's going to be a real challenge and we are going to need to see some innovations here to have that happen. So much still happens — I thought with cloud I would be flying less — but so much still, I can't stress this enough, so much has to be done face-to-face. You have this global compute utility, and I think because we're now crossing more political boundaries and geo-boundaries, that people really need to understand, can they trust that person that has my service in several times zones away?

Ashwin Krishnan: [00:14:29] You brought up GDPR, so I can't walk away from that. Clearly there is increasing awareness of what it is. But one thing that you're saying is the bipolar nature of understanding what GDPR is versus, "My God, what's it going to take for me to be GDPR compliant?" And then there's this famous thought that lots of people have, "Let's wait for the first 20 million euros or 4% of revenue fine to happen, and then I'll act." So, from your perspective, again you mentioned privacy and trust, are you seeing organizations starting to use GDPR as a reasonably, well-defined framework of this is not about compliance anymore, it's about doing the right thing? And is that going to push the bar, where you'll be having a conversation and say, "Hey, my job is to protect employee rights and customer rights and collect as little data as possible," or is this just one of those many compliance regulations that people just check the box and then hope that they're doing the right thing and that the auditors don't puke all over them when they come in for the annual audit?

Jim Reavis: [00:15:42] Yeah, that's a lot to unpack there! Let me try to do that. I do think that GDPR is definitely, at very high level, creating a cultural impact. Even though the European regulation does have a global impact, because everybody does business there, European companies and businesses that have lived this are really thinking through how they transform their IT and their business to focus on being the best in privacy as being a market differentiator for them and having that be something that creates business. It's not just doing the right thing because, unfortunately, I think that if doing the right thing is in conflict with addressing shareholders' concerns — there's a lot of corporate social responsibility that to me is a lot of hand waving — but I think they're actually starting to see that this is how we are going to attract customers. Particularly as they're getting younger, more savvy, and understand that, "Hey, this company respects my privacy." The scandals with social media, Facebook and others, and the big stock drop — maybe they've recovered, I don't know, I don't follow it — but that is sort of reinforcing that this is a matter of strategic business benefit for us to do this now.

So, at CSA we've been working with data protection authorities, we've created a code of conduct that says, here's some tools provided by CSA that can help you comply with this. We're seeing people being cautious, liking it, using it, but being very cautious, taking the same approach they did with STAR. Are we doing the right thing? You know, to be fair to people who are trying to comply with it, there's a lot in there that is not specified and articulated. There are so many questions, and when you ask a supervisory authority in Europe, "Well, what does this mean for my Wi-Fi access point that's collecting information, specifically what do I retain?" They answer my question, "Well, we'll let you know when you're in trouble." So, when the litigation happens we'll see; it's a real challenge here.  But I do think it is having a real impact outside of Europe as well as inside of Europe. We have to rethink this. You have to make privacy THE differentiator.

Ashwin Krishnan: [00:18:24] In that last point you mention the Wi-Fi access point collecting data. I think the conversation is starting to happen — which is a huge sea change — on where are these data collection entities, who are the data processors, and who is the data collector, and so on. Just switching gears, I know you're doing a lot on IoT as well. Talking about lack of standards, there's a huge playing field over there. This is going into a non-tech area with IoT, there's companies that are throwing out these sensors and data-collecting devices who have no tech background, per se. Are you finding it challenging trying to address that market? Say, I'm a small-to-medium company, and I know nothing about security, GDPR, or privacy, all I need is to be able to monitor energy used. So, what tack are you taking to address this non-high-tech community, but still using tech?

Jim Reavis: [00:19:28] We are all over the map honestly and starting up several different research areas inside of IoT. I'll be honest, I don't know if we're going to make an impact. When you talk about IoT, you think of it in terms of we're going to put a chip on every physical item in the world, which is the Marc Andreessen definition, how do you wrap your arms around that? A big part of the market challenge for providing security into this is we are talking a range of sub-penny sensors to an Airbus A380 or nuclear centrifuges. So, from an economics perspective, security will not be built into a lot of these. It's happening on so much of an industry-by-industry basis and, like you said, people with no knowledge of security there's a lot that's not going to be built in. There's going to be a certain economic range where you are going to be able to justify and be able to build in security. So, we're taking this approach of, "Hey, are there guidelines we can provide to build good, secure things?", but a lot of it needs to understand, and we have to be realistic, a lot of this is going to be very insecure, and so how can we deliver security? How can we surround that swarm of sensors with security? There's a lot of affinity there and cloud being the organizing principle on how you orchestrate IoT and thought computing. I think the cloud model is going to win, and the cloud providers are going to win in what manages the IoT. We reach out to all of these different groups and it's the same.

It's like the Groundhog Day of the .NET developers twenty years ago, when you would go scan the J2EE developers, and you would scan and break their applications and show them the multiple vulnerabilities. Oh my God, it's the same thing we're doing now with people who are building sensors or cameras or whatever else. And we're just going to have to see what we can do. It's like a Manhattan Project that's really distributed and we've got to look at it from every angle.

Ashwin Krishnan: [00:21:47] So, any last takeaways, pieces of wisdom, you want to impart to our listeners about being at Black Hat? What does success look like for you?

Jim Reavis: [00:22:00] I'd like to tell the security community that I think it's very important that we upgrade our skills and get more current. I see things like DevOps in continuous deployment that are potentially fairly transformational; DevSecOps, as well. We're doing a lot of things the old way. We're still patching things the old way. We have a lot of old models and we better watch out because in some of the immutable container, continuous deployment areas it's actually the developers making security decisions, and the security person can't even change any of it. So, we've got to upgrade our skills. We've got to be more forward-thinking and we've got to be looking at the blockchain. We've got to be looking at all the things. I started Cloud Security Alliance ten years ago and not a lot of people were thinking about this then and that's where we've got to be thinking about the things that are going to hit us and not just what's attacking my enterprise today. Those problems may not be around in a couple of years. So, what are the new problems?

Ashwin Krishnan: [00:23:11] Thanks a lot, thanks for the conversation.

Jim Reavis: [00:23:14] I enjoyed it very much.