Micro Focus Reimagining Cyber Episode #34 - Jim Reavis

Tue, 5/3 4:02PM • 36:31

SUMMARY KEYWORDS
security, cloud, organizations, people, CSA, understand, create, controls, application, cloud environments, CSP, building, trust, cybersecurity, cloud security alliance, Jim, vulnerabilities, company, industry, environments

SPEAKERS
Jim Reavis, Rob Aragao, Stan Wisseman

Read | Listen

Jim Reavis 00:00
Multi-cloud I think is just the reality that people find is having a competency and the bigger you are, the more you need to use different types of cloud-delivered solutions.

Rob Aragao 00:19
Welcome to the Reimagining Cyber podcast where we are short and to the point perspectives on the cyber landscape. It's all about engaging yet casual conversations and what organizations are doing to reimagine their cyber programs while ensuring their business objectives are a top priority. With my co-host Stan Wisseman, Head of Security Strategist, Robert Aragao, Chief Security Strategist. And this is Reimagining Cyber. So, Stan, who do we have joining us?

Stan Wisseman 00:48
Rob, our guest today is Jim Reavis, Co-founder, and CEO of the Cloud Security Alliance, founded in 2008. CSA is a coalition of industry vendors, stakeholders, and thought leaders that strive to create governance models within the broader IT community and the tech industry. For many years, Jim has helped shape the industry of information security and has been named one of the top 10 cloud computing leaders. Jim, it's fantastic to have you join us today. Can you expand a little bit more on your background for our audience?

Jim Reavis 01:18
Well, gentlemen, it's my pleasure to be here. And thanks for just being sort of a wonderful supporter of Cloud Security Alliance. So, you know my quick and boring story is I am kind of an older person, but I graduated in computer science back in the 80s and moved from working for a bank to enjoying the

technology more. And by the early 90s, I was doing a lot of systems integration, and the coolest systems integration and the early 90s was figuring out how to connect businesses to the internet. And the coolest, funniest, thing about that was all of the security problems you could see happening. So about 30 years ago, and we didn't call it cybersecurity then, but I guess cybersecurity now, and [I] have done a lot of different things typically have been an entrepreneur and built my own companies. And in cloud security lines, it certainly was a different one, we're seeing the issues, I saw that it was apparent that a nonprofit sort of neutral organization was very necessary to help lead us through some of the challenges that you could see were going to come about at that time.

Rob Aragao 02:33
Well, Jim, you know, many of you, including myself, view you as the pioneer in the area of cloud security. As you look back, you know, over those early days, what were some of the initial indicators that drove you to create the CSA, right? What was kind of that point in time, you feel that things started, click, and that, you know, maybe industry started realizing there's more to this cloud stuff, and we have to pay attention to the security aspects of it.

Jim Reavis 02:57
So, I think the definition of pioneers is the number of arrows they have on their backs. So, I guess I'm a pioneer. I think there's just I like the idea of standing on the shoulders of giants and the people that sort of influenced me. But you could see in just the early 2000s that this was coming in and the folks over at the Jericho forum were sort of the first that got on my radar that they talked about deep parameterization and identity and more of a virtual view and still in contact with a few of those guys like Paul Simmons leads our UK chapter does a lot of great things. And then Dan Gear, I'd say was a pretty significant influence. He wrote a book in the mid-2000s, which I think he wrote for a company he was working for, but it was just it was profound to me, where he likened the shift in computing to evolutionary biology. And the idea that it's not sort of a slow, steady-state of change. It's long periods of stasis, followed by these rapid flowering of new species and changes that he described as hairpin turns. And it came from, a Harvard biologist, I think, and he, at that time, was saying, “Hey, we've got all this connectivity. We've got all this data; we've got this virtualization that's happening.” And that's going to be very significant. And we're going to change to this more on-demand model. And then the third thing was there was a Harvard Business Review paper that was comparing IT to the electrification of America where, before we had a power grid, it was it was incumbent upon any business manufacturer to generate their electricity. And so, you would put your business alongside maybe a source of water and use that. And every organization had a vice president of electricity. And when the grid happened, and we had that electrification, you have this on-demand access to power. And that changed how our nation got built, and how manufacturing happened, how the business grew. It just changed, it was, you know, halfway through the Industrial Revolution, I guess, but it created this huge flowering. And the analogy, which probably is pretty apparent to people is, is while we're procuring and building all these computers, building these castles within organizations, but with the internet, now you can see that's sort of that grid that information grid, and now with the cloud, you could see that we're going to start optimizing, where we put compute resources. So, they don't need to be inside of a company that could be anywhere, and you could access them on demand. And going from a small number of people that have access to the capital to leverage compute that this was going to create just an explosion of information. And so, take taking that sort of sense that something big is going to be coming very soon,

that's going to change this model of how we use compute. And it's going to be very rapid, very dynamic. My thinking was, well, what do we do in cybersecurity, that's problematic, and it's that we are very hostile to change often. And I thought back to like, some of the conferences I went to and 2000, 2002, that timeframe, that one of the most popular giveaways were these Wi-Fi detectors, that cybersecurity people would go take into their office detect these rogue Wi-Fi access points. So, they can rip them out of the walls, throw them out to the people that installed them, burn them, and salt the earth. And basically, that made security people sort of irrelevant, not look like they were like enabling the business. So, the idea was, let's solve tomorrow's problems today. Let's start now before the cloud is very huge. And let's go create some very solid defensible best practices. So as the business is starting to use this going from pilot to production, the security people could say yes, that this is something we can support, we understand it, we understand how to map that to our view of risk management, everything else. So, the barriers, as you would expect, are just there are people that you must drag kicking and screaming into the future, there's a lot of fear about, you have a physical perimeter for your company, and then you have an information perimeter that extends far beyond it. And this fear that you're creating less security of a more insecure organization, when you do it right, as we didn't think it then. But we know now that you can create a more secure organization. So timing is everything. And a lot of great experts that again, I respect very much that have been very helpful and shown a lot of leadership along the way. And here we are, and we're in this new generation.

Stan Wisseman 08:28
And that transformation certainly has taken place now. I mean, it's one of those things where, when that, as you spoke to the some of the challenges that were initially there when CSA was first rolling out, a part of that value add was showing what the controls are that you needed to put in place to help understand how you can secure these new environments. And over the last 15 years, you know, we're basically to the point now where the accelerator is being pushed by most organizations and their cloud adoption strategies, right? I mean, it is enabling them now that help feels comfortable that yes, security and privacy can be addressed in these environments. That's no longer as big an obstacle. However, I'm sure there are still obstacles that we're facing, it may be different ones than we initially had, you know, 10 plus years ago. We're past those fundamentals. What are you seeing now is some of the cybersecurity and privacy issues that we still have to cope with?

Jim Reavis 09:27
So, it's interesting. And when I talk to a lot of enterprises and organizations about challenges, certainly, you find that the preponderance of organizations is cloud-first, or they look to the cloud for their new initiatives. But cloud is so varied right now. And you have the infrastructure, these hyperscalers where enterprises build a lot of their applications, and then you have SaaS where you're using essentially shrink-wrap software delivered as a service. And so, one thing you see that's just a big challenge is how do we harmonize our security framework and our security controls and make that consistent across all these varied areas. Multi-cloud, I think, is just the reality that people find in having competency. And the bigger you are, the more you need to use different types of cloud-delivered solutions. So that becomes a real challenge. There's, again, was, as you alluded to how things are moving very rapidly, as we look at things, it's this is the slowest things are going to be moving for the rest of our lives, it's just the change is accelerating. And so, you do find that that idea of being able to shift left being able to automate more, we're still behind the curve on automation, the level of compute

that we use is growing much faster than we're producing security professionals. And so that goes back to the hiring the workforce, side, a huge pain point for organizations to be able to do that. So, and again, the bigger you are the compliance framework if you're globalized, it's very challenging, we're seeing more and more that cybersecurity is national security around the world. And so that creates a lot of unique issues where data sovereignty having information in different countries proving that and being able to answer to a lot more masters than maybe we had before and again, at the same time, being able to shift left and stay very well aligned with the business. So, the challenges are there. And you can break it down, it goes into a lot of areas about how we run security programs, how we do software development, how we track vulnerabilities, how we track standards, and how we make sure we're consistently doing things. And the tools are, you know, I think very robust. But again, it's in a more dynamic environment. And in a perfect world, he gets six months to vet an application before you start using it, but we just don't have that luxury anymore.

Stan Wisseman 12:20
And just following up on that governance challenge. You know, there's the hybrid environments, multi-cloud, on-prem. And then you have the complexity of each of the CSPs. The good news is they've added a lot of cloud-native kind of security controls. The bad news is you have a diverse set of functions. So, you must learn, and your staff must understand how to do things potentially in AWS or Azure, GCP. And so, you know, ensuring that you're applying those controls, or the independent software vendor controls that would apply in those environments as well. That's a whole other level of complexity that can introduce gaps or weaknesses because you may not have consistency and visibility and understanding of how to monitor appropriately. But also, your personnel may not have that awareness, they need to apply those controls consistently.

Jim Reavis 13:20
Yeah, I would agree I, again, maybe going back to a little bit of history, one of the things that we were wrong about when we started Cloud Security Alliance, and I think the industry is this belief that, hey, the virtual machine is going to be this sort of atomic unit of computing. And it's going to be very easy to move your virtual machines or workloads around between different companies, different cloud providers, or even these ideas of there's going to be spot markets like commodities. It's not a commodity and what you have seen, and it's great, as you've seen, the innovation and all these unique services that the different large cloud providers are doing that are unique, and how they do server-based functions, how they do more abstraction and platform as a service and containerization. And so, it's to me, I liken it to the previous world of, are you a .net shop or a JDE-shop for your development? You're probably both, if you're big enough, and it's very important, I think, and it's very valued by organizations to have their people get that cloud provider-specific training and knowledge you should be a real expert if AWS is the direction you're going or if you're doing some of all you should get that that knowledge in combination with more of the neutral sorts of knowledge like some things we do and some others and take controls frameworks and try to see how they may apply to all these different technology areas. There's more we need to do to take have some sort of uniformity. It would be nice to have log files and things like that be more consistent across these different providers. But I think that's the whole value of an independent cybersecurity industry to create some of that harmonization because we're not, we're not going to get the major cloud providers to just sit in a room and say, okay, we're going to all do everything the same. Now, they're going to compete, and that's great. They're competing

on security, I was on a panel with Federal Reserve with Phil Venables, who many people know was Goldman Sachs for years. And now he's the CEO of Google Cloud. And he was just detailing all the investments they're making in security. And he was very gracious about the other hyperscalers. And, hey, we're all working very hard and competing to make security the differentiator.

Rob Aragao 15:54
Well let's kind of double click on that a little bit, Jim, because we've touched upon it a little bit earlier on that, you know, majority of organizations now it's a cloud-first methodology approach, you have some more advanced organizations that have been doing cloud for a while and are going multi-cloud, right, kind of hedging their bets, different service capabilities, applying better, you know, different test CSP models, which is fine. You still see through a lot of organizations that kind of inherently believe or think that they're going to receive in kind of the umbrella security coverage from that CSP that they're contracting with. So when you, you know, kind of think about that, what are some of the best practices that CSA yourself, you know, is going to drive, you know, kind of what are the key elements, you'd say that you have to take into consideration and kind of shared responsibility model some elements to understand, you know, it's not just hand over the keys, you think you're all set, it's a lot still back on you. And the onus of ensuring that you are securing your data, no matter if being in the CSP or multi-cloud environments, doesn't make a difference, it's still yours at the end of the day, it's your responsibility.

Jim Reavis 16:58
Now, you said the magic phrase, which is shared responsibility, because there's one, with certain people a lack of understanding that they do have a responsibility, which seems odd. Most people do understand there's a shared responsibility, but they don't understand to what level and what depth it is. And we did, on the request of a group of financial auditors, just a little study of our star registry. This was a few years ago, and I think it still holds is we found that the infrastructure provider satisfied about eight or about 15%, on a few of the case studies, we did have the control requirements, and the other 85% were the responsibility a combination of if you are doing all this work yourself, and you're building your applications, it's all yours. If you're contracting a SaaS company, then it's between the SaaS company and the customer, they have the 85% responsibility. So when you look at the definition of cloud, and you know, NIST did a great job defining that what we did is we sort of visualized it as more of a layered model, kind of like the OSI model, where you think of the SaaS software as a service, the whole business application that exists as layers on top of the platform as a service, which exists as layers on top of infrastructure as a service. And it's a bunch of APIs. And it can be, it can be several companies providing different services and APIs that deliver that full business application. So, it's like peeling those layers like an onion and understanding that taking the control framework and understanding which are the applicable things. So certainly, if you are, are developing a service inside of a cloud provider that the physical security of access to the hard drives, that's not within your purview, but all the questions about how you handle the data, the decisions you make, are you going to do multi-factor authentication, all those things. That's important to understand. And so typical large company, maybe they're working with three big infrastructure providers, and they probably have two to 10,000 applications, SaaS applications. That's where they've got to be continually looking at the, at a high level, the security of those SaaS applications. And for the infrastructure stuff they're building, they must build in almost all the security. So, you’ve just got to understand the type of cloud service we're using. Let's take the control framework, which is our cloud controls matrix, we try to break it down into that

there are controls that are relevant if you've got physical responsibility. This is if you are responsible for the provision eight of the users are or if you've got other responsibilities there that you can sort of break it down and, and kind of narrow the focus. But the message is, that you always have some responsibility, and it could be very significant for your use of the cloud.

Stan Wisseman 20:14
Jim, I want to pivot to the threats, we're seeing in the cloud environments. I mean, you have typical hygiene issues like, you don't set the permissions properly on your S3 storage, and therefore you now have granted access to those that you didn't intend to, right? You may have mentioned API and an API attack surface could be much broader than you expect, and threat actors can take advantage of it if it's not governed properly. What are you seeing as far as some of the difficult threat vectors hitting cloud environments? And how is CSA addressing these or recommending them to organizations? How to better address the newer threats?

Jim Reavis 21:08
It's a good question. And it's something that continues to be a challenge and how we think through this, but when we analyze here's all of the usages of cloud, here are the threat actors, here's where security is in place, we do find that almost all of the security problems do end up happening. The further up sort of the stack, I would say, you go, where users whether it's a SaaS company that's using this or more likely, even the cloud tenants, what they're doing ends up being a lot of hygiene issues, which you sort of talked about a few of those, and they may not have like very strong identity management, very robust, and it creates this risk of exposure and elevated exposure, you got to protect admin root accounts a lot more in the cloud environment, because they tend to have access to a lot more resources. And so that becomes important. We are doing a really good job with maintaining the gold code standard of the images we're using. Are we rolling these out in the right way? Do we have that sort of automated, you know, continuous deployment, and are we using things like cloud-based functions to roll back any changes that might degrade like the access control to the different virtual machines or other things like that? So, it's a lot of identity versioning patching, and finding the vulnerabilities. Understanding that doing threat modeling correctly for cloud, understanding where the vectors are different, we're not thankfully seeing at this point. A lot of what we fear is the sort of deep penetrations into the infrastructure providers and moving laterally in cloud hopping. We're trying to stay very vigilant and continue to do research in those areas. So, we try to encompass a lot of this is what we call our top threats section. And it's a great area, you can find it on our website, where we talk about the most common threats that, again, have a lot of these identity, hygiene governance issues; and then how to look at it, from a using traditional risk management and threat modeling tools, but understanding the different cloud vectors on how you should think about that. And that is tending to help quite a bit. And we're always going to be like, wanting to be very sophisticated. And we're trying to encourage from a threat intelligence perspective to see a lot more sharing between different cloud providers. And that can be harder, but between the tenants that are using these different cloud environments, because hey, what may look like an attack on an Azure and AWS or GCP, it may be happening and multiple of those and it may be an attack on a big bank that happens to be using all of those. And so, understanding those sorts of things are areas that are somewhat immature in the industry, but we need to work more there. But, you know, I find that organizations almost have all different sizes. If they focus on a lot of the basics in cloud hygiene, they can do very well because again, there's so much of it right now. That's

where the bad guys are going. They're there. They're not doing these highly sophisticated real hammer memory manipulation attacks, and we'll have to help providers.

Stan Wisseman 25:00
They don't have to, right. I mean, they can take advantage of the poorly maintained or patched, or configured tenants? And that's what they'll go after.

Rob Aragao 25:12
Jim, some of the kind of things we're hearing a lot about, and I want to hear your thoughts on it, how it applies to what you're seeing, from a cloud perspective. So, zero trust, right, we continue I mean, it's been around for quite some time, but the major emphasis especially since last year with the government sector, and the executive order is an example. The securing of the applications right, as we're migrating, again, within cloud environments. So, when you hear some of those kinds of topics, and you even talked about some of that a little while ago, kind of threat modeling is an aspect of the application side of it. But you know, what are you seeing as relates to those areas around zero trust and more of those security applications around cloud transformation?

Jim Reavis 25:52
So that's a good setup. One, I must thank you for that question. So, zero trust is something we're very passionate about. And that was an announcement we made at our research summit in March is a Zero-Trust Advancement Center. So, it's kind of interesting, because this has been around for quite a while, I think. John Kindervag at Forrester articulated this over 10 years ago. And he was basing that on some of the other things that came out of the government. And I think the Jericho forum that I mentioned previously, it's becoming so popular now because it was a little bit pandemic drive. You saw organizations that had, what they felt, very secure environments. And then they had to move these very secure environments, maybe multifactor authentication key fobs with their notebooks, and then they went home into these insecure environments and got the teenagers over there, you got the smart home that's potentially corrupting that, and that's where I think we, for me anyway, we started to see a lot more interest here. So, CSA's viewpoint on zero trust is, that it's kind of been captive of a more product perspective that these products will provide zero trust. And it's more of a philosophy and a strategy that if you cannot implicitly trust anything, then you have to go back and look at this, this system that you are trying to secure and look at those components and understand how you can create a strategy and an architecture that gives you enough built-in trust that you have confidence that these systems work. And so that's helping people sort of rethink things. Because if you are, for example, you've got maybe a SaaS application, that's a CRM that's got high net worth customers in there, you don't have control over that. It's a SaaS application. And maybe you've outsourced the call center that deals with that to another organization. So that becomes like, you understand there's a lot more of a human element. It's not, it's not down to like a network product, and how do we vet those, those people in the call center, and maybe there's a technology for exfiltration, and other stuff like that. So, it's just one example where we're trying to have people go back to think about strategy, think about philosophy, and then move forward there. But I think fundamentally, zero trust because now we've got so much technology and automation, zero trust is going to, at some point, consume all of the architecture of the Internet and, and cloud, I think we're going to be able to move to that model. I don't know how long that's going to take, but I fundamentally [think we’re] going to go there. So, we think that's, that's important. So, the

software question and how we think about that, we, the concerns we think about a lot are vulnerabilities. And, you know, we think we can improve software development. But this dynamic nature of it means we're always going to have vulnerabilities, we always got to have ways to manage that we got to have a lot of transparency into like the software bill of materials and things. But if you think back to like, the amount of technology we had, when, for example, the mitre CV program was started, I think, 20 to 23 years ago, and the amount of technology we use now, and the number of expected vulnerabilities versus the actual vulnerabilities we know about are hugely different. That tells us there's a very big problem and there are a lot of insecurities out there in our software. So, there's, that's, that's one of those, you know, all of the industry efforts that we're going to need to do to make that better and to solve that problem. It's not going to happen overnight.

Stan Wisseman 29:56
And that's a very good point, Jim. It's going to take quite some time to try to wrestle that one down. But you know, one of the great resources that the CSA established was the STAR program, which, again, going back to the beginning of the conversation help give those guardrails to help understand how CSPs cloud service providers can be more secure, and provide a level of evidence that they've put in proper controls, can you expand on the Star Program and the benefits it provides as well as where it's going?

Jim Reavis 30:36
Absolutely. So, the STAR program was based on this philosophy that we, one, shouldn't force and it's not sustainable to have software companies must respond to proprietary questionnaires, assessment questionnaires from every single one of their customers, which is kind of where the world was trending towards. And let's look at more of a shared model because those questions seem to be the same. So, so the idea is security achieved through transparency is a great way to do that. So, we built, we started with our control framework, the cloud controls matrix, and then our questionnaire, which is called the CIQ. And then the STAR registry is a way to create a multi-leveled approach where you can self-assess. And a lot of people say, well, is self-assessment valuable? But when you must be transparent about it, when you must publish it online, where everybody, your competitors, and your customers can see it it creates a fair amount of rigor. And then on top of that, we have this one called Level Two, where instead of creating our assessor network, we said, let's merge in our best practices, with either the ISO 27001 certification, or the SOC2 attestation project. So, all of those types of organizations that do those certifications, and attestations, could do one that is specific to CSA. And so that's what the STAR program consists of, we've got somewhere around 1800 companies in there. We would love to see more. But if you are a customer, this is something that's a free resource, it can greatly reduce the vendor procurement process, the assessment, the analysis, you can drill down and understand a potential service you're going to use, you can understand the security issues, and then you still may have some unique questions on your own. But it changes that from 100% to maybe 5% or 10% of the things that you need to follow up on. So free resource, we encourage people to go use it, if you are a cloud provider, and you're looking to maximize your market, you need to understand that a lot of enterprises require an organization to be installed if they're going to use them. So, it's a great way to show that, at the end of the day, what you're selling is trust, if you are a cloud provider, and to do that you're showing that you can be trusted. And it just reduces a lot of friction. And in terms of where we're going with it, we're seeing a lot more opportunities to federate and harmonize with other industries and

countries. So, the nation of Italy recently, which you know, they're a company of maybe medium-size USA, but instead of building their own FedRAMP, they’re using CSA STAR, and this is the level to the third-party assessment as this is the standard for whereby cloud services can be used by public administration ministries in Italy. And so we're seeing that there are other countries as well. We recently had an announcement that the Motion Picture Association, that there are partnering with us and there's a recent announcement from the Cyber Risk Institute, which came out of bits for the financial services industry, where the cloud controls matrix, our controls framework is central to the cloud protection profiles that they're creating. And so basically, what we are seeing is [that] STAR [is] federating and harmonizing a lot of other industries, nations without being a single standard, but solving that 80% to 90% of the problem and creating a really good path where hey, if you've done this, then you have a very small amount either if you're either on the customer side or you're on the provider side, to be able to address more unique needs to hit into Straight are a country's we're pretty excited about it. A lot of investment in that. And, you know, a lot of I think evangelizing we're going to need to do around the world, but it's going very well. And it's accelerating. I think we saw a 40% growth last year, and we're expecting about the same this year.

Rob Aragao 35:18
Well, Jim, that's great to hear. It's exciting to see that there's a program like that that you've established, but just the uptake, and as you just mentioned, right that, that great growth just in the past year, but helping provide some standardization, I think is critical. So great to hear that great to hear everything else, you must share in kind of the journey of establishing the CSA, the different things along the way, some of the latest things, and also kind of what your you're looking forward to and seeing additional aspects as relates to cloud security specifically. So, thanks for coming on. We appreciate it.

Jim Reavis 35:50
My pleasure. Thanks for having me. Thanks, Jim.

Rob Aragao 35:53
Thanks for listening to the Reimagining Cyber podcast. We hope you enjoy this episode. If you would like to have us cover a specific topic of interest, feel free to reach out to us and you can find out how in the show notes. And don't forget to subscribe. This podcast was brought to you by CyberRes. CyberRes is a Micro Focus line of business, where our mission is to deliver cyber resilience by engaging people, processes, and technology to protect, detect and evolve.