03 Trust vs. Cloud_Gerry-Miller_V2.mp3

Gerry Miller [00:00:03] If you think about the way that infrastructure is managed and the way that distributed applications are built today, there's a tremendous amount of shared risk. And so we've had to evolve regulatory models, we've had to evolve contractual models. The industry is tremendously different around security and risk management from a decade ago.

Jeremy Huval [00:00:30] This is episode three of Trust Versus. I'm Jeremy Huval, innovation officer at HITRUST.

Robert Booker [00:00:35] And I'm Robert Booker, strategy officer at HITRUST. Our topic today is Trust versus the Cloud. And the voice you heard at the top of the episode belongs to Gerry Miller, founder and CEO of Cloudticity. They are leading provider of cloud management, security and compliance services.

Jeremy Huval [00:00:50] And today on the show, we're tackling the cloud, what it enables for businesses its impact on compliance and risk, and how to interpret the ever present headlines of yet another cloud security breach.

Robert Booker [00:01:03] Jeremy, we've seen the cloud evolving almost continuously for a number of years, and cloud is not really a new thing. It's been around the way we've seen it for years and years, but organizations are still yet to go there. And as I think about cloud for a long time, I think about the work that you've done and your journey towards shared resposibility inheritance. Why is this topic even relevant when we're talking about Trust?

Jeremy Huval [00:01:24] Yeah, good question. And we thought it was worth giving a whole episode to cloud because as organizations navigate the risk management and compliance landscape and try to communicate meaningful assurances to their stakeholders. The cloud is either something that has dramatically changed the way they approach all those efforts or it's something that's about to. And thinking about where cloud is just the general adoption cycle and a hype cycle. We're definitely over the trough of disillusionment. We're leaving the slope of alignment, and I think a lot of companies are well into the plateau of productivity. People are either about to be significantly impacted by the cloud or they already have been. And with that change, compliance, risk management assurance is all to change too. So it's such a subject to navigate that there's way more content than we can cover in this episode, but is still warrants attention.

Robert Booker [00:02:22] It's such a deep topic, and there's really no fault as thinking about it as just a lot to consider. But Gerry makes it super approachable and I really like his approach a pragmatist about all things cloud. In fact, he's really the cloud optimist. If there is such a thing. I really enjoyed it and I think we both learned a lot and we both work in the space and let's get into it and hear what Gerry has to say.

Jeremy Huval [00:02:43] Yeah, can't wait. Let's do it. Gerry, you want to tell us about your company and a little bit on how it came to be.

Gerry Miller [00:02:52] We started Cloudticity in 2011, 2012 timeframe, and from the beginning we've had a singular mission of helping health care organizations successfully leverage cloud technology. Early in our formation, we recognized that managed services in general is a process. So if you're a center, you have to have people that are taking servers out of boxes and putting them in racks and pulling network cables. And what we recognized is that because we were cloud data from day one, that what most MSPs had to do with people we can do with software and better than a headcount problem, we view this as a software problem. I'm a software engineer by trade, brought in a bunch of other software engineers and we built a platform. Glad to see the oxygen that automates the vast majority of what most MSPs have to do with people. In the health care industry, that's really important because people make mistakes. Software, once you've debugged it, it works the same way every time, all the time. And so in a highly regulated industry, using software to manage the day to day is a highly reliable, highly auditable ability to align with regulatory

frameworks like HITRUST can be proven through analysis of source code, analysis of the automated logs that it generates. I think about the getting the basic definition right, because I think cloud's like many things, it can mean different things to different people. So if you're talking to a physician business leader or somebody that's not a practitioner or technologist, how do you define cloud? What do you what's your kind of go to elevator pitch on that? Ultimately, for an end user like that, it probably shouldn't even matter because what a practitioner wants or what a physician wants is reliable back end technology that doesn't break for them. And technology, ideally for somebody on the frontlines, should essentially be invisible. And so for a person on the frontlines, whether they're technology, whether they're PHR or they're interoperability solution or they're clinical solutions, whether that's running in a data center, in a cloud at some edge or some future technology, as long as we can make that technology as unobtrusive as possible, you know, at that level, it really shouldn't matter.

Jeremy Huval [00:05:01] So the cloud has been around for years and years. I think AWS launched EC2 back in 2006, over 15 years ago. And even your company when you started a decade ago, it's not new and the cloud is not new. And this concept of moving data into the cloud is not new. But man, when it first started, it must have been unthinkable that we were going to put covered sensitive data in the cloud, like health care data in the cloud unthinkable when it first started. There's an openness and a receptivity not only to cloud but the tech, the clouds enabling. What do you think's contributed to this change over time?

Gerry Miller [00:05:40] What we've seen change over time is that there's a growing acceptance across all industries that cloud security is probably better than any one company can do by themselves. If you think about AWS, Azure or Google, they manage millions upon millions of customers globally. And so their security has to encompass the fact that they're servicing so many organizations. And so the scalability of their security is always going to be greater than any one company can do on their own. Your stake in the industry a while to recognize that. But I will say that when we started Cloudticity 12 years ago, our very first conversation were always with the security teams. And today, that's not so much the case. We've definitely seen an industry wide acceptance that cloud is just going to be better. Now, that being said, there are instances of breaches where people have misconfigured their clouds and sometimes that gets mistaken for maybe cloud is insecure, but it's really how you use it, right?

Jeremy Huval [00:06:45] There's so much news about this cloud problem, this cloud breach, this cloud data leak. Like, for example, a global car company disclosed this decade long data leak exposing millions of customers data. Decade long, it was a, turns out root cause was a misconfigured cloud bucket that allowed anonymous access. Decade long it was out there. And then two weeks later they announced another follow up. Seven year long, same kind of problem. If organizations as big as global car companies and major financial services companies can have these kind of problems in the cloud, is there any hope for the rest of us?

Gerry Miller [00:07:23] I would argue that the problem is not with the cloud. The problem is in how we use the cloud. If you don't know how to effectively leverage the cloud investments that you've made, you have no hope of of security. But it's not an inherent deficiency in cloud technology. It's an inherent deficiency in how organizations are leveraging it. Cloud is not just another data center, right? It's not just somebody else is managing your infrastructure. The way that you have to operate in the cloud is very different from the way that you operate in a traditional data center. And so where we see problems like what you mentioned arise is when organizations don't invest in upskilling and reskilling to take advantage of cloud native services. And so it's not that cloud is inherently insecure, and in fact, it's significantly more secure. It's that cloud needs to operate differently than the traditional I.T. model. And when we see security problems, it's almost always a human failure, not a cloud failure. It's a human that didn't understand the inherent difference between a traditional data center and a cloud environment, and failed to do the proper configuration and then failed to put in place the kind of monitoring that cloud requires, which is typically different from the way that traditional data centers operate. The solution to that is that cloud offers the ability to automate infrastructure management. And many organizations that adopt cloud for the first time continue to do things manually, as they always did in the past. They've got a

lot of people looking at screens and they don't take advantage of infrastructure, automation, infrastructure as could automated deployments. Many of these concepts are foreign to those that have yet to operate effectively in cloud. And so we think that's much more a human failure than a technology failure.

Jeremy Huval [00:09:24] Do you think health care entity can expect higher or lower IT run costs after the move to cloud in general?

Gerry Miller [00:09:32] We tend to see cloud adoption start as a financial exercise, but quickly morph into an agility exercise because the real benefit of the cloud tends not to be cost savings, which is where companies tend to start. But the real benefit is agility. Like when we brought the first health information exchange onto the Cloud. We did that in 2013, I think, and the implementation timeline was 18 months, and we had that thing up and running in production in six weeks. When New York State was the hardest hit state with the pandemic. They came to us and said, "How many months will it take to build a data lake so that we can get our contact tracing program in place?" And we have that up and running in six days. And in six weeks, they went from being the hardest hit state in the country to the first state to cross green. If you think about financial ROI, the ROI on that project was tens of thousands of people didn't die. So very quickly, organizations start to recognize that the true benefit of cloud is not measured in dollars and cents, it's measured in agility and the ability to move not just twice as fast, but 100 or 1000 times as fast. And, you know, that brings tremendous benefit to organizations. But if you think about where we operate, which is the health care industry, that brings benefit to people and families, cities and states and countries. That's how we think about cloud, is the ability to have transformational impact on organizations.

Robert Booker [00:11:02] Yeah. There's a lot in what Gerry just said there. And you know what comes to my mind as I'm listening to him is that old meme or cliche that says there's no cloud, it's just somebody else's computer. And I know I've said a couple of times that early in my cloud journey, that cloud is just managed services of a different type. So I think we're right in acknowledging the misconception that many people think cloud is just another type of data center.

Jeremy Huval [00:11:25] Yeah, and muddying the waters even more is that you can treat the cloud like just another data center. If you don't know what you're doing or maybe you have to for one business reason or another. And what I mean by that is you can say install a database management system on a cloud server that you spun up and just treat it like an on prem instance if you have to. But if you did that, you'd be missing out on so many advantages that the equivalent cloud service has to offer. I think Gerry's view that cloud enables us to do in software what managed service providers and I.T providers have previously done with people is sort of a really pragmatic slice of this problem.

Robert Booker [00:12:04] Yeah, having a single management plane and everything accessible via API makes the cloud easier to audit, easier to monitor, better to manage compliance, blueprints, all those standards based goodness things that cloud [00:12:17]are MIS provide. [0.0s] Help you configure the whole environment a manner thats compliant to something like HIPAA, it gives you predictability towards your objectives and you know what you're trying to do.

Jeremy Huval [00:12:26] Yeah, and everything having an API is important because it allows interconnectivity and it lets you build against different services altogether, faster, easier. It's kind of funny that centralization of the management playing document and all these APIs and having everything have an API while made it easier to stand up and build against and configure it also sort of made it easier to target an attack. Because when you think about, I don't know, like an old iSeries box sitting on the corner of somebody's server room. The young bad guys today couldn't even get in if they had physical access to the box. But because like half of it's written in an old RPG, like where's the documentation for that? Right? Whereas all this stuff is been in the cloud, it's against known services, everything is well documented and there's a single API. So within inappropriate access, one script could nuke all your whole environment against all that well-documented stuff. So yeah, definitely good examples of the change risk landscape. I can talk about

it all day, but we have an interview to get back to, so let's pick up where we left off with Gerry. I was thinking about cloud adoption in the health care space and just how much clinical insights it's unlocked in terms of the individual patient care. If I was to think about that level of unlocking insights, is it that significant on the compliance, risk management and regulatory side as well? Do we have that much more data unlocked and insights unlocked about how well we're doing at securing our data in a cloud environment as opposed to on prem? Are the tools that much better?

Gerry Miller [00:14:04] One of the really cool things about managing cloud infrastructure is that it generates a tremendous amount of telemetry data. We can trace every single TCP IP packet as it traverses a virtual private network. We can trace transactions and and it produces more data than you could ever imagine. And the real challenge is if you have so much data around what is happening inside of your systems and how they're interacting with each other, what do you do with that? Traditionally, it relied on humans staring at screens and trying to identify anomalous patterns. But because these data are accessible, they're either pushed or they're pulling more by API. Cloud gives us an opportunity to build telemetry monitoring solutions that far exceed anything that could ever be done in a data center. And furthermore, it gives us the ability to build AI based responses to what we see in the real time telemetry of how our systems are operating in their operating. The ability to train models that use AI to watch what's happening and respond effectively. But more importantly, automatic is really a game changer in our ability to secure our customers solutions. Jeremy and I spent a lot of time in the world of compliance, the world of trust, the world of assurance. And we've talked for a long time about a concept of continuous monitoring. My experience, again, coming from a large company, is that compliance is viewed as a point in time. We assure report we have an assurance exercise and we think we're good and we can prove we're good and we know we're good. But you just described something very different, which is a way to keep it continually alive and continually forward looking. So I'm almost thinking about continuous compliance, continuous monitoring, continuous security. Does cloud allow us to get there and how? You're right in that, many organizations think about compliance as a annual or semiannual check the box activity, but a cloud just we've never thought about it that way, right? Because you might be completely compliant, which means that you've got optimal risk mitigation on one day, but if the next day you're not continually updating to address an evolving threat framework, you're not doing yourself or your customers or ultimately your patients any favors. So compliance really needs to be thought about as a continuous activity, not just so that we can keep, for example, the HITRUST logo on your website, but that you can really day by day continue to mitigate your risk, continue to address an evolving threat landscape, and ultimately continue to minimize the opportunity for threat actors to perform effective cybersecurity breaches.

Jeremy Huval [00:16:51] What kind of thought changes, mindset changes perspective leaves also have to happen on the risk management side of the house and start thinking about the differences and risks of an on prem IT presence versus a cloud IT presence. It seems like there'd be an equal shift in the risk management side of the house as well.

Gerry Miller [00:17:12] If we go back to your example of the automotive company. So in a data center, there's no concept of an object store like S3 and so the ability to misconfigured something that would make sensitive data publicly accessible is pretty limited. And what we have to recognize is in a public cloud, you have services that can be exposed to the internet if they're misconfigured. And so the way that a compliance organization in the security organization thinks about cloud has to transform equally as much as your application engineers and the infrastructure engineers. In a data there was no such thing, for example, as a shared risk model. And as soon as you move into the cloud, you're 100 percent at a shared risk [00:17:57]model. [0.0s] So if you just think about the infrastructure, you give up physical control of your infrastructure. And so you have to trust your cloud service provider that they're providing that deep level of security of the actual facilities in that they've got good power management and cooling management and access management. And when you give that up, how do you attest to your regulatory bodies that you have good physical access controls when you have no control over your physical access controls? So it was interesting when Cloudticity first got HITRUST certified, maybe six years ago. The first question our assessor asked was, "What's the address of your data center? And when can we schedule an onsite visit?" which is nonsensical in the [00:18:44]cloud, [0.0s] right? So I remember telling, "The

address is somewhere in Virginia. And no, you can't come to visit because AWS won't allow it." And that that really changed the face of how assessors like HITRUST really think about that shared security. We work really closely with HITRUST, and we helped define that original shared security model. We helped define the inheritance model so that when AWS invested in a HITRUST certification, we were able to inherit those controls from them so that we didn't have to attest to security measures that no longer fell on our shoulders. So the way that we think about security in a shared model from an infrastructure perspective has evolved pretty dramatically. And then if you expand that into the way that applications are built, we also need a shared model around application security management. For example, I'm not going to rate a text messaging component of my application if I want to write an application that reminds patients that they have an appointment tomorrow. A simple text message that says, "Hey, don't forget you have a doctor's appointment tomorrow." Is a very valuable thing to health care. But I'm not going to write a text messaging application. I'm going to use Twilio where I'm going to use Amazon SNS. But in that case, now Twilio has the phone number of a patient, and that's considered PHI. If you think about the way that infrastructure is managed and the way that distributed applications are built today, there's a tremendous amount of shared risk. And so we've had to evolve regulatory models, we've had to evolve contractual models. The industry is tremendously different around security and risk management from a decade ago.

Jeremy Huval [00:20:25] Yeah, I appreciate that. And the cloud shared responsibility model is been a journey, and I like to think that we're advancing the conversation with our share responsibility here in this program. What have we not talked about that you think should be on everyone's mind in terms of thinking about cloud risks and cloud security and health care technology?

Gerry Miller [00:20:47] The biggest thing that I can encourage organizations that are nascent in their cloud journey is just keep an open mind. Think differently. The way that we approach cloud technology has to be very different from the way that we approach on prem environments. And it's great to think about all these cool new things that we can do and we're going to move the needle in health care. It's going to get less expensive and more effective, but there's still a tremendous amount of risk. A health record sells for about 75 dollars on the black market, while a credit card number or a Social Security Number sells for about two dollars. And there's a reason health records contain everything about all of your personal information, your Social Security Number, your next of kin, and every address you've ever lived that there's a reason why it's the most attacked and most breached industry. While we are executing on these really cool initiatives to just make people healthier and keep them healthier, we can't lose sight of the fact that as we adopt new technologies and as we break apart our applications and distribute them across various technologies and ultimately various companies, the threat landscape will just continue to get more and more dangerous. And so we need to continue to evolve our regulatory frameworks. We need to continue to evolve our individual approaches to security. And we have to come at this brave new world with these security first mindset and risk minimization and evolving frameworks that were designed for in 1990's [00:22:27]air [0.0s] data centers. Just don't provide the level of risk mitigation that more modern architecture requires. And so really staying up to date with how regulatory frameworks and risk mitigation tactics align with an accelerating evolution of technology innovation is going to be critical to our success because it just takes one major breach to set us back a decade. And as an industry and as a collection of organizations dedicated to helping people's lives get better, we can't afford to have that happen. And so that constant vigilance and investment in both compliance and the security and risk mitigation that good compliance will generate has to be at the forefront in order to provide the foundation upon which we can build this next generation of health care capabilities.

Jeremy Huval [00:23:21] Appreciate that you indicated the need to evolve the regulatory frameworks and HIPAA has been around so long. There's been rumblings about how to revisit HIPAA on the regulatory side. Nothing's happened yet, but it's interesting to see where that will go.

Gerry Miller [00:23:36] It's certainly an exciting time in terms of the service that we have now have the opportunity to deliver. And at the same time, we do need to update our thinking about how

we've traditionally approached security framework. So I think you and I are completely in alignment on that.

Robert Booker [00:23:55] Thanks so much for the opportunity. Yeah. When we talked a few minutes ago, Jeremy, in our first break out, we were talking about how cloud change necessitated other big changes. Not just technology, but the way the company looks at finance, things like that. And Gerry brought up yet another when he talked about how regulatory compliance and control frameworks have had to change and evolve as well with the move to Cloud.

Jeremy Huval [00:24:13] Unfortunately, the wheels of big machines like those can often turn very slowly. Regulations focused on IT security that haven't been updated in decades are missing the boat around key risk areas of modern technology environments and controls frameworks that were designed for, you know, 1990's air data centers just don't provide the level of risk mitigation that the more modern architecture requires.

Robert Booker [00:24:37] It's so important that we stay abreast and rally around a controls framework and approaches that stay constantly updated to address new technologies, new threats, new risks, changes in the risk landscape, and to incorporate the changes that the regulators are making as they learn to pivot to these new technical approaches.

Jeremy Huval [00:24:58] Yeah, I'm hearing Gerry talk about just a small slice of the security capabilities and monitoring capabilities available in the cloud. It's difficult to argue with Gerry's point that cloud security is probably better than any one company can do by themselves.

Robert Booker [00:25:14] Yeah, and talking to Gerry reminded me of something much bigger than the security boost that we can get by moving to cloud. The true benefit of cloud is not measured in dollars and cents. It's measured in agility and the ability to move not just twice as fast, but 100 or 1000 times as fast. And that's that's a pretty exciting concept if you think about the opportunity that creates for business.

Jeremy Huval [00:25:37] Yeah, I agree. That was helpful for me to really appreciate the why and for organizations that have already adopted the cloud. We're like sure, we know all this, but I think there's more innovation yet to come. We're not done innovating on the cloud, and I don't think anyone has. Even if you been in the cloud a long time moving to things like serverless architectures lets you quickly spin up parts of a system without having to fight with getting new hardware and provisioning all the things that you might have had previously provisioned. And when you need a new part to a system, you don't have to build it yourself. It's just a service away. You need machine learning. Got it. You need single sign on or like multifactor as a service for that click, click, click done.

Robert Booker [00:26:18] And just thinking about agility broadly, you just the agility of scale, the ability to spin up and spin down and to, you know, put more compute on the floor when you need it for like a peak season or some big campaign. The world endured COVID 19, and I think about all the new things that we had to do to be reactive to COVID. And, you know, I think a lot of that would not have been possible using traditional IT. So just having IT be more agile, making it more responsive to the business, able to better serve the customers. And then from that last example, health care bringing benefit to people's lives. I mean, that's that's real. And when you put that on the floor in the right way, that you know, that that's going to make people healthier and save people's lives, perhaps even.

Jeremy Huval [00:26:59] I agree. And on that note, let's say goodbye until next time. Thank you for listening to Trust Versus presented by HITRUST. And thank you to Gerry Miller for sharing your wealth of knowledge on the cloud. Every episode would challenge trust and discussions across the world of security, compliance and assurance. We hope you join us again.

Robert Booker [00:27:16] Thank you all. Goodbye.