IT Matters - Episode 27

Thu, May 02, 2024 1:47PM 30:53

SUMMARY KEYWORDS

startups, soc, technology, companies, frameworks, security, type, service, cohere, solution, talking, darrell, team, give, space, business, partner, vendors, success criteria, reference points

SPEAKERS

Keith Hawkey, Narrator, Darrell Stinson

N **Narrator** 00:07

Welcome to the IT Matters podcast, where we explore why IT matters and matters pertaining to IT.

K **Keith Hawkey** 00:13

Welcome, everyone to the IT Matters podcast where we crack into the minds of the brightest IT leaders and discuss the challenges facing us today, so we can stay sharp and guide our organizations to a brighter digital future. I'm your host Keith Hawkey, a technology advisor and some might say IT whisperer. But enough about me, today we're discussing security compliance with the VP of IT and Security of Cohere Health, a software startup in the healthcare space. Cohere is actually the winner of the Triple T and has been named both Healthcare's Fierce 15 and CB Insights Digital Health 150 list, as well as ranked on LinkedIn's top startups. And today we have Darrell Stinson, he leads Cohere's IT and security, and he knows a thing or two about building security compliance plans for startups, as he successfully implemented at many young companies across the past decade. Darrell, welcome to the IT Matters podcast, how you doing, brother?

D **Darrell Stinson** 01:28

I am doing great, Keith, thank you for that very warm and eloquent welcome.

K **Keith Hawkey** 01:35

Anytime you have a call, just give me a ring, I'll type something up real fast and put a smile behind it.

D Darrell Stinson 01:41

Thanks so much.

K Keith Hawkey 01:42

Happy to offer off my services there. So Darrell, today we're really focusing on cyber security compliance. And one of the reasons I thought that you would make a great guest to have on is is your background, particularly with startups and and how you've been able to you know, startups typically don't have the most resources to and prior knowledge to adhere to some of the probably more prevalent today is the cloud focused compliance, startups mostly operated since they are starting a new company and getting into the data center game as most attractive as it was before. Can you tell us a little bit about yourself? How did you end up in the position you're in, a little bit about your career, and how you got where you are today?

D Darrell Stinson 02:33

Certainly, my start, was actually in the US Army. So Military Information Systems Security, that was my job in the military. I ensured that conversations or data that was supposed to remain secret, most things that had a computer chip in it, I was trained to repair those items. That's where I got my start. And that's where my foundation was built from the compliance space to encryption, algorithms, and rotations, all those types of things that we utilize today in the cloud, and SaaS, and platform as a service, data center technology and this was over 20 years ago.

K Keith Hawkey 03:17

I know that IT or technology in the Army is a little bit of a different beast than it is in the private world. How did you get involved in startups? I know that you're based out of Atlanta, and there's a active group of startup companies and a little bit of an incubator city. How did you land in and kind of so many startup companies? And can you tell us a bit about your path there?

D Darrell Stinson 03:44

Sure man. So after my time in the military, I did work as a department of defense contractor. So I did things like, teach binary math to soldiers who are joining the military, networking, and switching and all those things. This was in Augusta, Georgia at a base formally known as Fort Gordon, it's called Fort Eisenhower just recently went through a name change. But looking at the Metro Atlanta area. Yeah, you're right. There's a huge community here, we are so interconnected. It feels like there's only 50 of us, everyone knows everyone. But lots of startups or companies call Atlanta home for many different reasons, right. But my security engineering job was with a startup and it was in the healthcare space. And I was exposed to things that I had never actually seen in a private sector. Things like auditing on the SOC side, Sarbanes Oxley, writing policies from scratch, and implementing firewalls, virtual desktop infrastructure technology, I thought it was fascinating just a level of resilience. So that's where I cut my teeth on building things from scratch so staffing teams and figuring out the right people to hire. What

tools are good sometimes you won't always have the right resources or funds at startup to just throw money at any need or solution. You have to be resourceful and you have to be decisive. And that's one of the things that I love about startups, you get to solve current problems with current technology, and current willing and able bodies, right? I just love formulating these teams and creating new solutions that really take, you know, startups to the championship. I call it the promises.

K Keith Hawkey 05:21

Yeah, something stuck out to me, you mentioned they, you know, there's a lot of grand ambitions of startups, but you often have very limited resources, because they are focused on the monthly cost. And I've worked with with a handful of startups, and that's a primary concern, vast majority of services today, cybersecurity services, they have a monthly cost to it or an annual cost, everything is moving to subscription model. So you have to be extremely resourceful when you're taking on this challenge. Is it safe to say that you may have experimented with some open source technology? Have you ever had any experience with open source?

D Darrell Stinson 05:59

Absolutely. So open source is probably one of the first areas that companies that don't have unlimited resources would go to. What can I utilize that doesn't cost me either anything or a lot of money, that still helps me solve my problems or address the need. So open source tools are very useful at times. But sometimes you can find yourself limited for certain reasons where you need to step up your game, and maybe subscribe to a particular tool on a monthly expense, or maybe the annual expense. And this all comes with maturity of growing companies, right? I've been in all different spaces. So financial, technology, healthcare, data center, I mentioned the military operations before, but getting exposed to a number of different types of domains and industries, has really helped me put together my repertoire of solutions that I can go to and lean on when it comes to maybe something that's similar. Maybe it will help us in this this particular stage.

K Keith Hawkey 07:00

Yeah, cross pollinating, especially in the technology space is is so vital today with with the rapid pace that an IT leader has to has to keep up with. So let's dive into some of the framework, some of the strategies that you've implemented, when you walk into a new company, new startup software space, what do you typically find as far as the ecosystem? And how do you go about starting that process of what are we complying to? What are my resources? How do you start your methodology?

D Darrell Stinson 07:38

That's a good question. So I love when I have the opportunity to utilize auditing, right, or some sort of reference point, for instance, in the healthcare space. So we have high trust HIPAA, that gives us guidelines or reference points on what we should be doing, or need to adhere to. But

there are other frameworks that many of us can use almost any company, and at any phase or any level of maturity. And it's the five elements of a cybersecurity framework, those five elements do go in order. So let's identify, protect, detect, respond, and recover. And then I'll kind of talk a little bit about each of those and why they're important for their own reasons. So identify is the main question that you asked me, right, you want to identify what's at stake? What business you're in? What type of staff do you have? Or what type of correspondence documentation policies do you already have on hand? Maybe you have none. Maybe have some or maybe it's elaborate. But you also want to identify physical and digital assets, talks about ecosystem. Most companies are they have some sort of whether it's a hybrid remote work, setup, or like Cohere remote first, and folks are all over the country. Right. So that identification piece is really important, because you need to know what you're defending, what you need to protect, what's at stake, what's critical, what's not. And through that discovery, you'll probably find that you have some blind spots, too. So lean into the next element of this, which is protect. So you wouldn't defend a $10,000 asset with $500,000, for instance, right?

K Keith Hawkey 09:21

So let's, I'd love to get into that a little more. Because what you're talking about is very persuasive when you're trying to illustrate the numbers to the decision makers of business.

D Darrell Stinson 09:35

Absolutely.

K Keith Hawkey 09:36

It's one thing to say that we have secured these elements of our business, we have protections in place, we have these layers, but it's far more persuasive in my experience, to describe the value of the assets they have. And then compare those to the security tools and the cost associated with those to protect those assets. Do you have any specific examples of, of doing drawing that comparison? How do you value data value various assets within a company.

D Darrell Stinson 10:12

So someone like myself won't usually dictate that to the business, right? And we encouraged and this is where the collaborative effort is really, really important because you can't do IT or security alone. But what we what I usually encourage the business to do is understand the value of the assets, if we're talking about HIPAA data, right? What is the cost of a breach? There are some reference points there, right? What is the cost of a breach? What are some of the fines or penalties that we may be held against, right. Maybe you're in the banking industry, there are reference points out there that can give you dollar amounts. And then maybe some of those investigative efforts or forensic efforts might be required to investigate or the you might have to devote to it. If you understand some of these numbers and I've often partnered with firms that come in and do a benchmark assessment, it can help you decide exactly, hey, it would cost you this amount of money based on the amount of data that you have, the types of resources that you have, if you experienced a breach in the industry that you're in. If you

experienced, experienced a breach, it would probably cost you this much money. And here's your level of maturity to defend against it. This is one of the first things I like to do it at a new organization, sometimes it's a little pricey, but the amount of visibility that you get, and understanding your maturity, what it may cost you or may not cost you so that you can have the right kind of conversation about what we're spending and how we're investing in the program. But a lot of it, Keith, is analysis. So once we understand some of these reference points, we don't want to spend, you know, $1.2 million dollars on investing in a breech and paying out in fines. So it makes sense to spend maybe a quarter of a million dollars on this particular resource that helps us carve out supply chain, and vendor partnerships. And maybe we create a hybrid team that allows us to have staff on hand, and vendors in like a 24/7 type of scenario. There are lots of companies of vendors who offer SOC as a service or manage detection and response. And a lot of companies think that, well, if you hire a couple of good security people, you've probably covered something goes wrong. It couldn't be farther from the truth, right? What I like to do is create a maybe a hybrid scenario. So one of these SOC as a service teams think of it like an ER team. So someone comes into the ER, and you have someone who's checking blood pressure, someone who's doing maybe chest compressions, someone's who's dressing a wound, but everyone does something, right. And in the SOC as a service piece. That's what companies want is assurance. So put a price tag on there. And you say, well, we could spend x amount of dollars, whether it's 100,000 or 200,000 on this and we have coverage, we'd have assurance, something happens at three in the morning Christmas Eve, we have a team or a solution in place. And that kind of helps paint the picture to either the board or executive leadership teams who need to make decisions on where money is spent.

K Keith Hawkey 13:14

Sounds like you've had to evaluate a handful of those SOC as a service MDR providers.

D Darrell Stinson 13:20

Yes, I have and have some implemented before. That's not the only type of solution. But there's so many different scenarios. And I think analogies that really, really helped me articulate or communicate to folks who don't have the depth and an understanding into IT and security space, but still need to know enough to make decisions. So that's kind of been one of my secret weapons.

K Keith Hawkey 13:43

There are seems like hundreds of SOC as a service providers today. And every MSP seems to be adding them to their list of services. There are names popping up doing it differently. Some of them are using SIM, some are not, some of them will simply rely on rest API's into existing infrastructure and ecosystems. How do you kinda sniff out what MDR providers are worth the value compared to some that might be cutting corners, right? Because that's a common issue when you have a newer IT leader that's confronted with everyone saying the same thing on you know, with demos and calls? Have you learned learned any tactics to ask their MDR provider to see how they compare to some of the better ones in the market?

D Darrell Stinson 14:36

Oh my goodness. So it's not just SOC as a service or MDR. This works for almost any solution that's new to the business. You know, one maybe you're not so familiar with. I call them science projects, but it's a proof of concept, right? So you need to hold a proof of concept. Maybe there's a problem statement or here's the gap that we have today. Right? And maybe it's not still clear in the beginning, but you have a pretty good idea. And then you develop success criteria, the ideal solution would give us 24 By seven coverage, it would give us coaching in an event that we needed, it would give us forensics or investigation in the event that we need it. It would give us triage, of alerts and events that are happening at all times of day, all across the business in our infrastructure, you figure out what that criteria is, right. And then you invite stakeholders. So you shouldn't make this decision or do this science project or POC in a vacuum. So if you have security engineers, and they hold a conductive proof of concept, maybe a week or two, maybe it's a month, but they run through the concept, and then no one else has been invited. So platform hasn't had a chance to look at it, engineering hasn't had a chance to look at it. Other folks who may be impacted by the alerts or invited to an incident, something happens, they haven't had a chance to weigh in. I invite everyone I can invite to the party. So they can ask questions, they can maybe add success criteria. And then you deliver this or take this to the vendor, or the candidates, maybe you have three, maybe you have five, you need at least two, I suggest three, you kind of boil it down. And then you compare them across that success criteria. Maybe it's price, maybe it's speed, maybe it's ease of use, or usability rather, right? You figure out what's most important to you as a leader for the team. But then that really benefits and provides assurance to the business. Once you do this, you will discover, hey, this actually doesn't perform the way they promised. Or maybe it does more than what they promised. They have different things like Slack integrations, and you can get notifications more quickly. This proof of concept we should do it for every new solution should almost never be done in a vacuum. And also that communication piece of it helps build your credibility, helps build your buy in and people are more inclined to support decisions that you make. So that is my cheat code, not just for SOC as a service or MDR solutions, but almost every spirit that I that I take to the business.

K Keith Hawkey 17:13

Yeah, and it's a great way to identify potential gaps, because often we're on demos, and we hear something and we comprehend those words in a particular manner. But when it comes to having to manage the solution, it's an entirely different experience. And even on a demo, you know, if you're on four or five demos a day, if it is your seventh meeting, you're back to backs, and you're trying to pay attention and comprehend brand new technology, you're likely to miss aspects of the service, especially something as important as the eyes that are going to watch over your data. And it makes sure that your organization is secure.

D Darrell Stinson 17:59

Absolutely. One of the things that is really big about the proof of concept is at the end, I have partnered with vendors before I take the price tag to the business, maybe I'm boiling it down to one or two. We work together on a day. And a really good partner will work with you on the content of that day. Maybe put one together based on your particular use case or implementation, things that work right for you. When you're talking about SOC as a service in particular, you're also talking about scaling a team and a startup cannot hire, you know, 20

people on one department in one month, especially in security. So it will carve out what it costs to bring in a SOC analyst, how much work they would do, how many of you might need, turn it into a dollar amount, and then the business can make really solid informed decisions, it makes sense to close this gap with this particular partner. And yeah, you're right. There's like 100,000 different vendors in every single space of technology today, especially security. Trying to sniff all them out is really hard to do. You can't you don't have enough time to meet with them all. And your business partners internally don't have enough time to review them and give you buy in. The proof of concept kind of accelerates the decision making, clears the smoke and mirrors, and it gives you a level of peace of mind too, in saying that I lean on this, I believe in it is the right thing for us, and here's why.

K Keith Hawkey 19:28

Yeah. And and I could see how there are very specific challenges in the startup space. Considering a vast majority of your data is stored in a SaaS application potentially, maybe you're leveraging Azure or AWS initially GCP or another Iaas cloud solution. You know, a lot of your infrastructure is housed in some sort of co-managed situation made servicing customers with large cloud environments, the primary offering. And with that, from an architectural standpoint in mind, it sounds like sussing that out early, especially when you're within your company has a lot of focus on the cloud is important. You know, there are all occasion, providers in space they've been around for a while. They're good at what they do. But some of the cloud integrations can be limited, because they're having to retool, and they're having to hire resources that do resources to manage the cloud space and to manage that service. What are some of the strategies that when you are having to adhere to like SOC two, type two compliance? What are some of the compliance requirements that you've had to adopt? And get a startup in line to in your career? And do you have any words of advice and maybe things that you've learned during that journey?

D Darrell Stinson 20:56

So I've done about 25 audits in the last decade. So the ranges from ISO 27,001, ISO 27,017, and 18, SOC one and two, type two, Sarbanes Oxley, I've done multiple of these at different startups, right. So when I say championships, and promised land, this is usually what I have in mind when I join these these different companies is to bring them to a position or posture that is comparable to either competitors or other players in the space that provides or establishes a level of assurance. But the benefit for folks like me is exactly what you mentioned is those guardrails, I use the frameworks to tell the business the direction that we should go. So here's our Azmuth. Here's our Northstar, whether it's high trust, or SOC, or ISO, or NIST, we pick these frameworks together, maybe it's required at the business, maybe it's driven by contractual requirements. We can't sign these customers unless we achieve ISO by this day to maintain high trust. When you sift through those controls and those frameworks. They've ranged from 114 controls in an ISO audit to upwards of 280 in a high trust audit, right, which I've done about seven high trust audits as well. Maybe that 25 number's a little off, I need to recalculate that. But anyway, that is what I use the guardrails, right, just like a roller coaster, or just like a train, we will adhere to ISO we're will we will adhere to high trust, whether it's how we review accounts, how we baseline our laptops and endpoints, how we monitor activity and traffic that traverses the firewall, how often we review firewall rules, what we do when it comes to supply chain and vendor assessments, vendor management, how we engage in incident, right,

conduct that lifecycle. But on the engineering or software development space? What's our software development lifecycle look like? How do we handle approvals and changes change management, all these things are built into the these frameworks one way or another. Sometimes the wording of the legalese is a little bit different. But this is what I use. My X Factor, though, is always connect with legal to help me translate some of the requirements. Think about, like GDPR And some of those that are highly highly wrapped in legalese, you need a good partner that will help you translate and say, well, here's a requirement And what it actually means is x, I can then take that and say, well, we can solve that problem, or we can address that requirement with security. We can facilitate privacy with security tools. And here's how we do it.

K Keith Hawkey 23:52

Yeah no, it really does. One thing that comes to mind as you're going through all the policy and process and laying the foundation, building the documentation, the framework of how your company is going to comply with whatever compliance that they need to, have you experimented with any of the AI platforms in doing this. I've spoken with a number of IT leaders that have and some have found success. Others are more skeptical, as how much have you dabbled into maybe the Chat GPTs of the world or the Azure AI are some of the other ones to help us?

D Darrell Stinson 24:35

Yeah, so I'll tell you this. We're currently in a phase where we are exploring artificial intelligence solutions, and how they can either help us accelerate certain areas of business, help us optimize some of the operations that we have in place or help us with accuracy. And so we're at a place where we're evaluating those right now. So that's actually where we are.

K Keith Hawkey 25:00

On leveraging Chat GPT I feel like I'm using it more and more for a variety of things.

D Darrell Stinson 25:06

Short answer is yes. Right. So artificial intelligence can do so many things we have just they feel like we have no idea all the things it can really do. And we're probably using it for in situations that are not optimized, but I have dabbled in in Chat GPT personally, and I've used it to do a lot of different things like helping to build frameworks for decision making, or you can use it for for different presentations, right, maybe there's a pre presentation that you want to deliver. And you can prompt Chay GPT to give me a presentation for a CISO, who's going to the board and wants to talk to the board members about security posture, right. It's gonna give you an outline and then you can go and sprinkle Keith in it, you can go and sprinkle Darrell in it and fill in the blanks with the things that are appropriate for either what your posture actually is or the things that maybe you would not have thought about to share with executive leadership or board members. Yes. Think of the time savings of receiving those types of frameworks from Chat GBT, the outlines, that's hours, that could be hours out of your day. To write a job

description from scratch, right? Yeah, you could totally Google your way through it. You could partner with the people team or HR, maybe they're busy at the moment, but you just want to get an idea. Give me a job description for I don't know, a VP of IT and Security. It's going to give you something to work with.

K Keith Hawkey 26:38

That gives me an idea. With everyone's busy schedules at work and trying it can be such a pain to bring the relevant parties into the discussion of the new technology. Some of them might think it's tertiary to their job, or it's low on their priority list. And they are already quite swamped with meetings and everyone that they're managing. I wonder if we could leverage a generative AI platform to ask is someone in this position with these responsibilities? How would they think about this technology that we're looking to bring in? I'll wonder if there's some data that we could feed into a Chat GBT to give us some idea of how they would view the new technology that we're introducing into the company, to get to just start that process, maybe be able to meet them where they are mentally, because, you know, we're all in our own silos we all will mostly think and consider the future based on our experience, Chat GBT, I'm saying Chat GPT, I know there are others, I probably use Chat GPT the most. That might be an avenue to help us realize other perspectives. And start that process.

D Darrell Stinson 28:01

I think that's brilliant. Someone like myself, it was one of my biggest challenges, meeting folks wherever they are. Because we don't make the decisions or make purchases, or limitations, we're siloed. We need to partner with either finance team or we need to partner with engineering, or we need to partner with legal or board members to sign off improve on certain changes, especially if we're talking major architectural expenses, right. But being able to frame those conversations or frame those topics in a in a way that is digestible for folks who don't have your level of visibility and understanding of the industry consequences even that's probably one of the largest pain points for folks in my position is maybe we see a consequence, we often think breach first in closing gap or solving the solution. Now we're talking about SOC as a service earlier, and being able to frame that in a way that folks understand the need, the value in executing or implementing the solution and why we don't want to be on the on the wrong side of not having made that decision. You got to make it easy, because you usually don't have a whole lot of time. And if you explain too much it's just gonna get lost in the sauce, so maybe using generative AI to to help us frame those conversations is actually a really good idea to experiment with that.

K Keith Hawkey 29:24

Words of the wise from Darrell Stinson. Don't have your message become lost in the sauce. I think that's an excellent point to leave on here as we end the podcast. Darrell, this has been incredibly insightful. Where can our listeners find you if they wanted to ask any questions about your experience or maybe receive some guidance?

D Darrell Stinson 29:47

I am very active on LinkedIn. So it's Darrell J. Stinson, CISSP, CEH, if you type all those things in you'll definitely find me, find my smiling face. Send me a DM, send me a connection, I'd be happy to reach back out to you.

K Keith Hawkey 30:06

We'll make sure to add those into the show notes. Darrell, thank you immensely for for coming onto the podcast and I certainly have appreciated the conversation.

D Darrell Stinson 30:18

Keith, thanks for inviting me, it was like having a conversation with a friend.

K Keith Hawkey 30:23

I like the sound of that. Likewise, take care everyone, have an awesome rest of the day and don't get lost in the sauce. We'll catch you next time.

N Narrator 30:34

Thanks for listening. The IT Matters podcast is produced by Opkalla, an IT advisory firm that helps businesses navigate the vast and complex IT marketplace. Learn more about Opkalla at opkalla.com.