#219 - The Professionalization of CISOs (with Steve Zalewski & Tyson Kopczynski)

[00:00:00] **G Mark Hardy:** Hey, on today's episode of CISO Tradecraft, we're going to cover something that's probably got a lot of you CISOs wondering about. Are we ever going to professionalize our industry? Are we going to be able to have some sort of standard that we all meet? Well, I've got two gentlemen who are going to tell you exactly how it's going to happen.

Stay tuned.

[00:00:14] **G Mark Hardy:** Hello and welcome to another episode of CISO Tradecraft, the podcast that provides you with the information, knowledge, and wisdom to be a more effective cybersecurity leader. My name is G. Mark Hardy. I'm going to be your host for today. And I have a couple of guests that are going to get into the details of the concept of a professional association.

of CISOs. And I've got Tyson Kopczynski, Steve Zalewski, welcome to the show.

[00:00:49] **Steve Zalewski:** Thank you, Mark. Pleasure to be here.

[00:00:51] **Tyson Kopczynski:** Pleasure to be here. Mark.

[00:00:53] **G Mark Hardy:** we were talking a little bit earlier, we had a call a few days ago about the concept of a professional association of CISOs, which I think is [00:01:00] rather, interesting, because like most of us consider ourselves to be professionals. However, there is an In this crediting body, like there is to say, I'm a CPA or I'm a doctor or an attorney or something like that.

and so let's start a little bit of a background, perhaps, how'd you come up with the idea? was it your idea or are you just along for the ride of how do we make us a profession, so to speak?

[00:01:27] **Tyson Kopczynski:** Wow. That's a really great question. to be honest, it actually didn't start in that corner, per se, the, corner that it started in was, really around how CISOs themselves are increasingly, Falling afoul, not falling afoul, that's probably the wrong term, but increasingly having more and more personal liability with regards to their job and their role.

Really good public examples of that are with Joe [00:02:00] and Tim. and their trials and tribulations that they've encountered over the past couple of years. And when you think about what has now occurred around this thing called the Professional Association of CISOs, it really started, as a conversation among CISOs, and, literally, I believe, the first, or one of the first conversations, or at least something that was more structured, was at RSA last year, where they came together and started talking about, hey, how can we create a insurance product, to better protect us from a liability standpoint.

So PLI product, and that conversation then continued at the Team 8 Summit, with an unconference session that was, ran by, Charles Blauner. And a group of CISOs where it then morphed from, Hey, we need to protect ourselves from a liability standpoint to a, no, we actually need to professionalize what it is that we're doing and [00:03:00] actually have something that is standing behind us.

Supporting that aspect, and so that's like the genesis and then it went forward from there into like further conversations further roundtables to fall of last year where a group of us came together and started actually standing up the structure. And then October, we were stealth mode.

We had some founding members that joined us. and then in November, we took the wrapper off, we had a very public statement on, this is what we're doing. and here we are today, obviously chatting to you, about what it is that we're doing.

[00:03:38] **G Mark Hardy:** Interesting. Yeah. So for most of us know the, fates of, for Joe Sullivan and Tim Brown, they have, led in, in a way they discovered that being a CISO does offer some pretty dangerous legal traps. And, even if your organization chooses to keep you around or defend you, you might end up with a fantastic amount of legal bills, [00:04:00] even if you're adjudicated to be innocent.

And so the whole idea that is how do we de-risk, if you will, from a personal perspective, the role of a ciso. Because I remember when those two cases came out, there was a lot of discussion about the chilling effect It may have in our career paths where a lot of us saying, Hey, I don't mind doing this job, but I don't wanna be the person gets shot at because you come.

Become the chief incident scapegoat officer. And that's not a fun place to be. And so you've talked about the development starting there at RSA and the idea, Hey, maybe we should protect ourselves. And then it's morphed now into almost an organization. So beyond just being able to go ahead and do like a group policy, okay, Hey, there's a whole bunch of us.

And so now we have buying power to get insurance. what is the value, if you will, for someone to say, Hey, I want to be part of this.

[00:04:49] **Steve Zalewski:** So this is where I came in. So with Tyson and Heather Hinton, they had obviously started down this path and then they approached me and I joined. And this is where [00:05:00] my focus is the practice of cybersecurity for 30 years, which is what we were doing, okay, and the creation of the CISO title. Is one that even today, you can either anoint yourself or appoint yourself a seesaw, right? And that seesaw word has now propagated into a whole different set of things. A field CISO, a retained CISO, an operating CISO, right? And so the question we were then tackling is, if we're going to now take this from the practice of cybersecurity to the profession of a CISO, that means we really do have to establish some basic understanding, rubric, and competencies and levels of what the word CISO means.

So we go back to, we got to establish a definition, but we have to measure against the definition, right? And that's what makes [00:06:00] the profession. And now, in opening that kind of door, we're now working through the, if you're a field CISO, right? Or you're a retained CISO, or you're a virtual CISO, versus you're an operating CISO for a Fortune 50, or you're an operating CISO for a small or medium enterprise.

Okay, how do we look at all those things and evaluate them on a common plane to be able to now realize What is it that a business is looking for in a CISO, and how do the CISOs themselves, put themselves in front of an accreditation process, not a certification process, right? And so now you see where we are moving forward to is lots of the community has certifications. is pass a test [00:07:00] and what we're saying is similar to the American Bar Association and the American Medal Association or the CPA is it's not about memorizing content. It's about demonstrating operational expertise as well as theoretical expertise in a way that we measure it equally. And now everybody understands what it means to be accredited as a CISO versus certified to have taken some CISO courses.

[00:07:31] **G Mark Hardy:** And a lot of these courses, were developed long before really CISO became a hard career path. And so I was privileged to teach at the SANS Institute for almost a decade. And I was their lead instructor for their 512 and their 514 courses, which are today now branded as leadership courses, and they're really focused on providing CSOs with the skill sets they need.

I have not looked at the current curriculum, but I will imagine there's probably a lot that's still in common with what was there [00:08:00] before. And this is not at all anything negative about SANS. They do a great job of holding extraordinarily high content, both for their instructors and for the course authors, to be able to deliver.

Excellence each time. But the question comes down to, as you had said, ultimately, you're passing a test and the San says are open book. You bring your five books, you build an index and the idea of indexing that thing hopefully puts enough in your brain that you can get through the test in the time allotted.

Because I used to tell my students, the good news is it's open book. The bad news is it's open book. So if you don't know what you're doing, you'll time out. But here, by instead of going for the certification. Okay. I've got a whole bunch of certs. You see them off of everybody's name. Now we're going to go ahead and have a different approach, which I think makes really good sense.

Now, if we take a look at, for example, change healthcare. that incident that happened, I think Senator Whiting had some comments that they might CISO it was not well qualified. the problem is that the government [00:09:00] may step in and tell us what to do. Some of the first efforts that took place are back in 2009 with the Rockefeller Snow that they had proposed going ahead and putting some controls.

But part of that was we, the federal government will tell you how to be in your career or words of that effect. some people, if they want to go dig out through 15 year old. proposed legislation, they can find it. Remember my friend, Steve Northcott, he was at the time was the president of SANS and we get to know each other pretty well, which very much against that.

I was a few times, one of the few times I wrote to my U S Senator, and said, Hey, I don't think this is really necessarily a good idea because increasingly the regulators, the government, someone's going to try to define a qualification and hold responsibility. So by taking the leadership role that you have.

You're avoiding potentially the problem of somebody else defining what it is for us, and then it could be potentially an ill defined standard because, quite honestly, the expertise of creating a CISO standard probably does not [00:10:00] exist within the halls of Congress today. good for you on that one.

So let's go back a little bit in terms of liability, and you talked about liability insurance. Where are we seeing the direction of that going with to cyber?

Because my I see my policies, my small business policy say, Oh yeah, we're going to start to exclude more and more things from coverage, which is, that's the stuff I really want to cover.

And so insurance companies are not in the business of writing checks or in the business of cashing them. So how do we go ahead and look at the direction that we're going of liability insurance perspective on that?

[00:10:36] **Tyson Kopczynski:** Yeah, so that's a good question. So around the liability front, with regards to what the association was focused on, we actually worked with, a carrier to construct a specific policy just for CISOs themselves. to cover them, right? So it's not covering the company. It's covering from a personal standpoint, the [00:11:00] liability that you encounter with regards to your role itself.

the policy itself, is actually quite good because we help negotiate the terms. The trade off is, the underwriters are looking at the association. as a method to evaluate the risk, right? So it's a combination of what your current role is, and then how you're interacting with the association because we're trying to define what the bar is with regards to being a CISO, including the kind of standards and ethics by which you're practicing.

So very similar to a doctor, right? you have a perspective of doing no harm and you sign up to that. the underwriters are seeking that element with regards to CISOs and seeking some methodology by which to evaluate that they're actually qualified for their jobs. and so the insurance product kind of goes hand in hand with that.

[00:11:55] **G Mark Hardy:** Interesting. And so the idea then is that the insurance companies say if you can [00:12:00] certify that somebody is at this level of proficiency to a level that we accept, and they say, our risk is probably much lower, much in the way that if you go ahead and you have airbags and anti lock brakes and passive restraint systems on your car, you'll probably get a lower rate because they expect you to be injured less statistically, right?

Then if you were missing all those things, what's interesting, and I'm wondering because I wasn't part of those conversations is do you get any pushback for the insurance companies or they simply said, Hey, thank you for doing our homework.

[00:12:36] **Tyson Kopczynski:** sorry, did we get pushback?

[00:12:37] **G Mark Hardy:** Yeah. Do the insurance companies say, your terms are ridiculous or do they say, Hey, this is a really good, thought out approach.

[00:12:45] **Tyson Kopczynski:** no, they've been very collaborative with regards to pulling this together. and again, the There are a couple of products that have emerged, the ones that are not associated with what we're doing over at the association. [00:13:00] No, no pun intended. actually don't have as good of, let's say, policy terms.

as the one that is actually done through the association, meaning you have to be a member, you, have to have signed the code of professional conduct, and eventually there's going to be some tie back to your point around the risk analysis to the accreditation process itself. and so now they've been very supportive, with regards to why this is important and, how they're viewing the, risk equation and evaluating, the right, underwriting these particular policies.

[00:13:37] **G Mark Hardy:** Interesting, a quick little war story. So wow, it's 25 years ago. So year 2000, a friend of mine, Mark Fabbro and I, we went door to door in New York city, talking to some of the insurance companies, they were saying, Hey, we've created an assessment that would allow you to go ahead and for these companies who are this new product, you have the, computer security.

Because I think we called it cyber back then, even, and we would assess them and let you know what the risk is. And if [00:14:00] they scored at this level or better, it means they've got the controls in place and therefore you can charge them a lower premium because you'll have lower risk. And oh, by the way, they can pay for our services because the premium discount is going to be greater than what we're looking at.

It's a win, win, And they looked at us like we had three eyes. I. Why would anybody do that? Of course, here we are later and you find out that if you're too far ahead of the curve, you're a heretic, but all of a sudden when the world catches up with you. So again, there is an effort, as I had mentioned over 15 years ago to do this at the government level.

But now you guys are doing that. Now you, do you think it was just these two CISOs who had problems or do you see, a potential. Seed change, if you will, in the way that attorneys, government agencies, shareholders, et cetera, are going to view CISOs as being a soft target.

[00:14:52] **Steve Zalewski:** That's already happened. See, but what, we're realizing is it's been happening for 20 years. [00:15:00] But it's like beneath the

waves, okay? The individual CISOs, as they reach certain levels of maturity in organizations where that accountability, okay, is now raised that they're at the executive level and they get hit with these types of events, they're lonely, right?

They're one man on an island. And what we're realizing over time as we've been talking within the community is it's a lot more common than people think. And so now it's time to leverage that knowledge, right? And what we're doing now is to be able to look at the 10 percent of the population that's been impacted.

And given that CISOs now, whether it's regulatory dictated or not, the executive teams in many cases are telling the CISO, we want you to sign off on risk. Your name goes on that paper, but we're not necessarily giving you. The risk mitigation through [00:16:00] insurance to manage that similar to what we do with our other named executives, D&O insurance as an example, and that's where we said so if it's not just the fortune 50, right?

It's actually much broader than that How do we bring insurance to the community so that the larger community can leverage this now as a negotiating option? As they're accepting this additional responsibility for their job without having the corresponding luxury of the risk mitigation, right? That many other named executives in other roles and companies have.

[00:16:38] **G Mark Hardy:** Now, do we see that these policies are going to be dependent upon the individual or the entity? For example, although somebody may become accredited, if they're with a small nonprofit and the most damage you can do is 100, 000 as compared to a fortune 10, where you can add a whole lot of zeros there, do they simply say, Hey, let's just go ahead and here's [00:17:00] your policy.

It will, here's change back from your dollar, or is it going to be something that says one size fits all.

[00:17:08] **Tyson Kopczynski:** no, you're probably going to see some stratification with regards to how they construct these policies. and it's also You know, based on the amount of coverage that a CISO is going to be seeking, because again, it's based on their personal circumstances and what it is that they're trying to protect, not what they're trying to, not what the company is trying to protect, hence the personal aspect of the policy, right?

so it is probably going to depend. the other aspect, or the other thing to consider is this is very early, right? this is a brand new thing that, that literally has just come online. and to Steve's point with regards that this has been happening like

under the current, for a very long time, in a sense the dam is also broken in [00:18:00] that you have these very public cases that have emerged that now more folks are going to realize that CISOs themselves are, targets, right?

They're soft targets. and so that, in a sense, compounds the urgency with regards to us organizing as a profession, because there's ultimately safety in numbers, right? If we are not standing up for ourselves and we're individually encountering these trials and tribulations, you're not going to survive, right?

especially considering the dam is broken, and it's probably going to become increasingly more prevalent, to go after the CISO with regards to accountability.

[00:18:45] **G Mark Hardy:** Now, this sounds like a great idea if we're going from a standing start. Okay. So I'm a private pilot. I have my pilot certificate. I did meet a gentleman in the 1990s. Who had his [00:19:00] pilot certificate signed by Orville Wright himself, because he got his ticket in 1931. And they said that Orville Wright, who was really the first director of what we call the FAA today, was the, only guy who never legally required to have a pilot certificate because there was nobody qualified to sign his ticket.

All right, I get that. the guy's name was Judge Spain, by the way. I'd like to learn more about him. He was very, old back then when I met him, I think it was in his nineties. And so we like caught up with a little piece of history. But today. We've got a proliferation of CISOs, some that are extraordinarily well qualified and well trained.

Some of them have just said, I are a CISO. They open up a little matchbook cover and on one side you can drive a long haul truck and the other side you can become a CISO. And that's where they went there. But how do we go ahead and deal with the fact that all these people are out there? Do we, have a, Little admission test.

It's almost you have to have three certs to you have to be this tall to ride, or is the accreditation [00:20:00] process not going to require any of those external certifications, but will it be completely self contained from your perspective?

[00:20:09] **Steve Zalewski:** That is where a lot of the thinking is going in, right? Because as we peel back the problem, that's exactly what we're realizing is. For people that want to be CISOs that are on the career path. Okay, then we've got to establish the attestation accreditation processes to give them the on ramp right and the stages to go through so we're thinking through with that Okay, but when's the last time a new professional association?

the ABA or the AMA or the, CPA have come forward, right? So this is not common that we're establishing a brand new profession for cybersecurity. So the question becomes, what do we do, with all of the individuals for the last 20 or 25 [00:21:00] years where we're trying to create an onboarding process for them?

That isn't start at the beginning, but that as fellows, they've been well established, right? People know it, that they go through the process in a lighter weight and are part of the leadership team to help us to continue to refine the accreditation and attestation process for the ones that are coming forward.

So we really do have those two stages. of the challenge we have right now and we're using, senior leadership in the security industry to work with us as we establish this process and you go through it to realize we do, we have a chicken and egg problem, which is we have to jumpstart it with senior leaders that people acknowledge, understand the problem for the first classes of looking to be CISOs or [00:22:00] CISOs at certain levels to be able to jump on.

So that is something we have been really actively working with and that's why we said is when you start to look at the word CISO and all the ways it's being used, establishing that spreadsheet of what they are versus what they need to be has been really foundational here is we're starting to let people see, just the fact that I can drive a car.

The ability to drive a minivan or drive a sports car is very different. And right now, everybody just is simply saying, I have a driver's license. And we're saying, that's not good enough now. These are the gradients.

Tyson, you want to add in on that? Because

[00:22:45] **Tyson Kopczynski:** no, I think that hits the head on the nail. look, at the end of the day, you have to start somewhere,

you look at doctors, like doctors have [00:23:00] been, doctors have been a profession for How long right? when you look at the process that they go through in the US to become licensed, it's 150 years or something of that nature, right?

And to Steve's point, these things don't happen very often. and there's going to be this gray zone while we sort out what it is. But that's also been the challenge point, to your point of, or the discussion we're having about people being on

their own island, right? we really, as a profession, haven't come together and said, This is what it means to be a CISO, right?

And these are the things that we need in order to ensure that we're successful, right? We need a definition of the role. We need a way to verify our skills and expertise. We need, insurance to support us. we need, a lobbying aspect to ensure that the right regulations are being [00:24:00] passed. we need other support services, whether it's from career development, to being, to you name it.

And the fact that we're starting to come together, the fact that we're starting to organize, I think that's actually the most key kind of monumental thing that is occurring right now.

[00:24:18] **G Mark Hardy:** Yeah. And there's a bit of a precedent. So I remember back in 97, might've been a little bit before that, Hal Tipton came up to me and said, G Mark, you need to get one of my certifications. It's called CISSP. And you'll have letters after your name. It's like, why would I give you a couple hundred dollars, but letters after my name?

of course he was right. I was wrong. It did catch on. And so I finally, caved in and did my CISSP exam, 25 years ago this month. So I've got a, I thought it was interesting is that they were increasing the numbers by 10, 000 every month to make the numbers look big, because if you took it before 2000, you got a four digit number, and then, 10, 000 series, 20, 000 series, dirty little secret, maybe, but we compared numbers with my friend and she did [00:25:00] Here's the month before and hers was 100XX and mine's 200XX.

In any case, the idea was what? Is that the CISSP was groundbreaking in so far as there really were no certifications for cybersecurity executives. Today there's a plethora of them and there's a whole constellation of different entities. They compete against each other as well as perhaps collaborate with them.

And there's always a whole My cert's better than your cert, and things such as that. Do you see that, based upon your success, you're the pioneers, so you'll catch all the arrows, so to speak, to allow everybody else to come in and settle peacefully after you have gone ahead and figured out where all the problems are.

Do you see a balkanization of this in the future? Or do you anticipate that maybe people will say the American Bar Association, we don't have 27 versions of a bar association. There's one. What are your thoughts about that future?

[00:25:57] **Steve Zalewski:** from my perspective, [00:26:00] certification, right? And a lot of it's been technical in the past, and now it's managerial. Is an important first step in establishing a profession because what you're starting to do is to say, what is the content that you have to understand to be able to do the job? And we've got good 2025 years now of different educational components or sans or others, right?

Building courses that look at a particular problem, technical, managerial risk, right? And provide background. Part of what the Professional Association of CISOs is saying, all of that knowledge is important. But how do you describe the discipline, competencies, and which are required at which stage in the maturation, of the types of CISOs that you are?

So that all of that certification is [00:27:00] still incredibly important, but we as a non profit now are giving people the ability to look at all of that and apply it against an accreditation process. To know, not necessarily the order, that too, but the practicality of what they need to be able to then go in front of a body of your peers, right?

With a very clear definition of the competencies and the levels of expertise you need to be able to be accredited to you are a CISO at this level and have demonstrated the ability to execute in these types of environments. So we see this as very additive, which was We're moving up the pyramid of now establishing the next level of maturation that would have been difficult without all of these certifications to establish the body of knowledge that we're now trying to organize.

[00:27:57] **G Mark Hardy:** Interesting. Okay. So for example, in my military [00:28:00] career, I'd had the privilege to serve in command. A number of times. I actually had nine commands over the career and the smallest command I had when you're a lieutenant or lieutenant commander isn't all that big. Then you end up with a major command where you have hundreds or thousands or in one case over 10, 000 sailors and you're still a commanding officer, you're still a CISO using the parallel, but your scope of responsibility is much greater and you look for the seasoning and the expertise.

You're not going to. Put a young lieutenant in charge of 10, 000 people when you've got people who've been around for 25 years who, who know that. So you see that as we go from a CISO, someone joining and they accept the code of professional conduct, which you've talked about before, then it can register.

and then they can do the attestations and then finally accreditation. We can talk a little bit about this flow of a little bit. is that then a, okay, here's my ticket. I can go hunt for CISO jobs. I've got my [00:29:00] insurance, or do we see this as coming out to be almost like, okay, you've done really well at this level.

Now, here is a, you're cleared or you're certified, almost, going back to the pilot's thing. Okay. I'm, I can fly a single engine land. If I want to fly multi engine, it's a different endorsement. If I want to be an airline transport pilot, it's a different endorsement. We start putting endorsements to say, Hey, we're going to endorse you to be a fortune 100 CISO.

But you know what? You're not going to get that a year after you got your CISSP, which was two years after you got your undergraduate degree.

[00:29:34] **Tyson Kopczynski:** Yeah, I think that's a way to look at it, right? It's akin to, again, when you look at like a, doctor, right? A doctor, they'll go to school to, to learn about medical stuff. they're gonna go take that knowledge then and apply it through a residency program. and then as they emerge from the residency program, they're, and again, I'm simplifying the process by the way, [00:30:00] they're then going to go seek a license to practice as a doctor, typically within their own practice.

and and they also have specialization, paths that they might want to take, right? Maybe they want to go be a heart surgeon versus a, kid doctor or so on and so on. you, in a way, could probably view what it is that we're doing akin to those types of similarities, right? we're viewing it as, yes, you need to accumulate knowledge, but there needs to be a validation with regards to your ability to execute on that knowledge to say that you're a CISO for this or a CISO for that, right?

and that's the, findings answered. it stops short of licensing, right? Because You can't really do licensing unless you have some sort of governmental body that's involved and blah, blah, blah, blah, blah, but if we don't, back to that, if we don't take the narrative in [00:31:00] our own hands, we could have the government come to us and demand certain licensing requirements that are completely outrageous, right?

[00:31:08] **G Mark Hardy:** And that was what we talked about from 15 years ago.

[00:31:11] **Tyson Kopczynski:** That's Right. So the point being is we, have to do something here, right? There's many things that are coming together at this

particular point of time, that if we don't come together as a community, someone else is going to do it for us, and we're probably going to be in a much worse position.

[00:31:31] **G Mark Hardy:** So let's go ahead and run with this and say for someone who's watching or listening to our show, Hey, I'm interested now before I sign up and, join, what would my experience be? So I know you've got different membership and accreditation levels. Do you wanna talk about that briefly, or, I could have got the slide up here, but I figured you guys know your material better than I do, but I try to do my homework.

[00:31:55] **Tyson Kopczynski:** so from a membership standpoint, we are very, early. There is only two [00:32:00] membership levels. One is, what's called friends. think of it as you're just showing support and you're trying to get insight into what's going on, right? So you get access to the membership level or the membership area. We publish things and we talk about, okay, this is what we're working on.

Then there's the events that are going on, et cetera, et cetera. General member is, where you actually sign the code of professional conduct. and you then have access to the PLI product. you have access to also do the attestation, process, which is coming online. and you're going to start having access to other benefits, like access to, legal console, to career support, to well beingness, being support, et cetera, et cetera, as we continue to build stuff out.

Over time, there will be additional membership levels that we will seek to develop, which actually is going to be tied to the accreditation progression, that folks go [00:33:00] through in order to become an accredited CISO. Steve, do you want to talk about kind of accreditation a little bit further underneath, with regards to how we're building out and thinking about things?

[00:33:10] **Steve Zalewski:** to Tyson's point, once you join general membership, the way we're thinking this through is there are three stages after that. You can be an associate CISO, meaning if you think about it like lawyers, you can be a paralegal. And so therefore you are a CISO, but you may be, or a CISO on the path. So maybe you run the GRC program for your company.

Maybe you're the architect for the company. Maybe you're the deputy CISO. So that you have operational expertise, right? But you don't necessarily have the full responsibility for the program. Okay. Or in this case, maybe you're working for a small company that doesn't have. as much of a risk profile in your

expertise can be limited [00:34:00] compared to being, a fortune 50 CSO size of the program.

So we call that associate, like paralegal. And then we have the attestation. An attestation is about demonstrating that operational expertise that you've been building as an associate. Has reached a level that it is across the 10 or 12 competencies, not just technical, but business, risk, leadership, management, okay, that you have the confidence, to, to enter certain verticals as a cybersecurity, maybe retail, maybe healthcare, or certain sizes of companies.

Okay, so that you are comfortable from your perspective as to the breadth of your knowledge and what type of environment you're good with. That's been validated so that everybody's understanding this is the sweet spot. And then you get finally to accreditation. [00:35:00] And in that case, what we're doing is we're saying, taking all that operational expertise and overlaying that with the right strategic kind of theoretical.

Expertise that you've demonstrated that you can be dropped into any environment, not just the ones where you have operational expertise, but you truly are right at that level that you can confidently be dropped into any environment and you knew how you know how to. Okay, establish and run a really good program.

That's what we're thinking about. That's how we're positioning it we have actually on our cohort two, so we've done a first cohort for the Attestation stage so from an associate CISO signed on general memorandum taking them through Attestation we're doing a second cohort now just kicked it off that for RSA, we anticipate having the second cohort through.

And now what [00:36:00] is we built the engine because those cohorts that have come through can then set up when we establish the ultimate attestation stage, right? Because now what we're doing is leveraging that experience, leveraging those first generations of, very capable CISOs to be able to help us build the program.

So to Tyson's point is crawl, walk, run, right? But what we're doing is thinking through the entire program and the stages and maturation. So everybody sees how it makes sense. And now we're getting the larger community to work it through with us, but it's not just theoretical. We are actioning and executing on this, right?

And so in the last six months, going from, Ground zero to where we are has been an awful lot of very satisfying work by a whole lot of people who all generally agree It's this is the time so we are the lightning rod to facilitate these [00:37:00] conversations But more than that, we're executing on the conversations

[00:37:06] **G Mark Hardy:** Got it. So we're covered a lot of ground here, and we're getting down to the last couple minutes of our show. So if somebody says, hey, I'm intrigued by this, and you say you've just started on your second cohort, full disclosure, I'm a member of that. If someone says, hey, do I just sit back and wait till RSA, as you had mentioned, and see what goes?

Are there gonna be a big release at that point, saying here we are with a big fanfare? Or is there a way that people can go ahead and go to your website and learn a little bit more and maybe interact with your team a little bit? particularly those who might say, Hey, I've been doing this a while and I've got some good ideas you might want to consider.

How would they go forward with that?

[00:37:43] **Tyson Kopczynski:** Yeah. So it's quite easy. You just go to the CISO. org.

[00:37:47] **G Mark Hardy:** TheCISO. org.

[00:37:50] **Tyson Kopczynski:** That's right. and you can apply for, membership. Now, the thing that I want to emphasize is this is for CISOs by CISOs, and [00:38:00] we encourage active participation. So as we continue to spin up and figure out the things that need to get done, we're actually having CISOs embrace building and running these things.

and so there are many, ways to get involved and push this forward. You just have to take the first step and actually get involved.

[00:38:24] **G Mark Hardy:** All right. So theCISO. org would be the place people can go. that sounds wonderful. So what should we expect then, on the 28th of April, as you had mentioned, I think that's going to be RSA. Is this going to be?

[00:38:37] **Tyson Kopczynski:** Yeah, so it's, April 30th. It's the Wednesday of RSA. We're having our first, CISO summit. it's adjacent to RSA.

[00:38:49] **G Mark Hardy:** like B sides, right? You'll be across the street.

[00:38:52] **Tyson Kopczynski:** Yeah, in a way. but it's purely focused on CSOs. we're having an all day summit. the [00:39:00] morning is going to be more general networking and a panel discussion, but in the afternoon, we're going to break off with a set of CSOs to actually have working sessions.

to work out solving things for the profession, right? So it's a little bit more unique than I would say a regular event because the idea is for us to actually get things done. harken back to the olden days of RSA in a basement.

[00:39:28] **G Mark Hardy:** Very interesting. And, Steve, any further closing thoughts you might have?

[00:39:33] **Steve Zalewski:** so to the audience, as Mark said, he's part of cohort two, so he's part of the solution with us now. So please feel free to reach out to Mark, right? And

[00:39:42] **G Mark Hardy:** are very good at delegating, aren't you? Like flick it, you go take,

people who are interested. you can go to our LinkedIn page for CISO Tradecraft. Let us know your feedback on that. And that's a great place to have a conversation back and forth with the number [00:40:00] of your professional peers.

I

[00:40:01] **Tyson Kopczynski:** Absolutely.

[00:40:02] **Steve Zalewski:** for active feedback, right? Be part of the solution. Because we either figure out the solution or somebody tells a solution, as Tyson said, and that is not where we want to be.

[00:40:16] **G Mark Hardy:** agree.

[00:40:17] **Tyson Kopczynski:** we don't. We need to take the narrative and control our own destiny because if we don't, I'm pretty sure we're not going to like the outcome.

[00:40:25] **G Mark Hardy:** good insight. gentlemen, thank you very much for being part of CISO Tradecraft. As we always try to go ahead and provide information to our viewers and our listeners. so Tyson Kopchinsky and Steve Zalewski, you've been wonderful in terms of giving us a little bit of insight into the CISO.

org. If you like CISO Tradecraft, don't forget to follow us on LinkedIn or Go ahead and subscribe to us on any one of the podcast channels. We're on almost every one of them, plus YouTube. So you can go ahead and see our smiling face when we want to at some point in time. So hopefully you'll find that this is a great addition to your [00:41:00] career.

If you want more, go take a look. We'll go ahead and put in the show notes, the connection for it. And we thank you for being part of our CISO Tradecraft audience. Until next time, this is your host, G. Mark Hardy. Thank you for listening or watching and stay safe out there.