Brian Contos: Welcome to the Cybersecurity Effectiveness Podcast, sponsored by Verodin. The Verodin Security Instrumentation Platform is the only business platform for security that helps you manage, measure, improve, and communicate security effectiveness. I’m your host, Brian Contos, and we’ve got a really special guest today, joining me is Richard Seiersen. Welcome to the Security Effectiveness Podcast, Richard.

Richard Seiersen: Hey, Brian. Thank you so much.

Brian Contos: Hey, Richard, before we get started, why don’t you give the folks a little bit of background on yourself?

Richard Seiersen: Sure. So again, Richard Seiersen. I am currently the SVP and CISO at Lending Club. Prior to that I was the VP of Trust and CISO for Twilio, and prior to that I was the general manager and the VP of cybersecurity and privacy for GE Healthcare and then a bunch of other things. On top of all of that, I have written a book called How to Measure Anything in Cybersecurity Risk, and I am currently feverishly working away on my second book as well.

Brian Contos: Wow. It’s fair to say you are not a security newbie, and certainly happy to have someone with those credentials on the show. So, Richard, give us a feel for what you do as a CISO and some of the things that are top of mind for you.

Richard Seiersen: Sure. This will sound, I guess, fairly basic, but as a CISO, I really focus on the people, process and technology. You probably think that’s not unusual to hear, but I’m always focused on what’s the team that I need to build given the particular company and what it’s trying to get done and where it is in its stage of development and where it’s located, too. Actually, that’s a really critical thing when you go about building teams, right? The last two being here in San Francisco.

Richard Seiersen: Beyond that, really I’m trying to understand do we have the right capabilities and trying to focus on do those capabilities work, right? So, you’re talking about process and technology there. But really focusing on, again, given the business and risk drivers that a company has, again, do we have the right capabilities in place. Are we thinking about the right things. Then again, really critical to me is, are the things that we’ve deployed, are they really doing what we expect them to do.
Brian Contos: Yeah. That's a huge one I'm hearing a lot, and I really like how you just didn't play lip service to people, process and technology. As we all know, when people generally say that, a lot of the times they mean 99.9% tech, and they go a little bit light on the people and process side. But you really doubled down on the people side. That's, I think, so critical, especially here in the Silicon Valley where it can be challenging to find people. They're really in high demand.

Brian Contos: Richard, you've written a book. Congratulations on that. It sounds like you're going in for it again on a second one, but tell us a little bit about your first book.

Richard Seiersen: Sure. So, the first book, again, is called How to Measure Anything in Cybersecurity Risk. It's the second book in a series. The first book's called How to Measure Anything, written by Doug Hubbard. Great, fantastic book. I think it's the number one book in business math and science 10 years running in Amazon. So, it's a generalist book in terms of measuring top stuff. Became a friend and actually a customer of Doug's a number of years back, and we had a friendship and mutual shared interest in all things quantitative.

Richard Seiersen: Continued to grow where we decided, "Hey, let's really write a book. Let's take the things from How to Measure Anything" ... Actually, he wrote two books, How to Measure Anything and The Failure of Risk Management. Let's take some of those concepts and with some of the concepts from the things that I have worked on and let's bring that together to the security domain. It's done well.

Richard Seiersen: One word of advice I'd give to anyone who is thinking about writing a book, unless it's the next Harry Potter, make sure it's something that you love, right? It's a topic that you love. If you were thinking that gosh, this is going to make me rich or world famous or anything else, that's probably the wrong motivation. It should be something that you love and where you're hoping to learn in the process because it's a lot of work.

Richard Seiersen: I also should add the book actually has done fairly well. It's actually required reading now for the Society of Actuaries exam. You actually as of 2018 can't do a test without having read through and comprehended material from our book, and I think that's really great. It's really great to see that security, and it's the only security book that's within that corpus, it's really great to see security concerns expanding into that realm. I'm pretty excited about that.

Richard Seiersen: The book's also increasingly becoming required reading in universities. I'm actually going out in October to help at Carnegie Mellon as adjunct faculty for their DoD program actually. I'm actually going out to Texas A&M shortly as well to do the same sort of thing, to actually present to their faculty and others on the topic of measurement and cybersecurity.
Richard Seiersen: The only reason, again, I bring that up is that we're starting to see security, particularly security from more of a CISO's perspective, more from a measurement perspective, more back to that topic of capabilities and validation. We're starting to see that, again, there's a scientific interest. There is a pure engineering interest, and it's growing in academia. It's growing in business, and I'm excited. I'll get off my soapbox. It's just exciting for me to see our world expand.

Brian Contos: Yeah. No, it's really exciting. Hey, congratulations on everything you're doing with Carnegie Mellon, et cetera with that first book. I think it really speaks to the importance of the topic. I mean, people have been talking about risk measurement and metrics for a while, and I think there's been a maturation in our space amongst not just CISOs and security folks but also business decision makers that might not be security savvy or even technical, CEOs, board members, et cetera, that are now concerned about this.

Brian Contos: They use KPIs and measurements for everything, so there's an expectation to say, "Hey, I need some measurements for what's happening in security." A lot of times security folks just aren't armed with that. What are maybe two or three sort of like "aha" things about the first book that you might be able to share with the audience? Just maybe things to keep in mind for anybody that's going down this path of saying, "Hey, I do want to start measuring and start validating and getting real metrics out of my systems."

Richard Seiersen: Gosh. I have three takeaways really from that process. I speak on this topic a lot, and these are takeaways that I actually inherited from Doug in his book and have applied to our realm. But it's really being clear on what the concept, object, and methods of measurement are. I think, again, a takeaway is something conceptually, like someone who is listening, what ideas can I give that will allow them to really think further.

Richard Seiersen: When we speak of the concept of measurement, I mean, most people probably think, "Oh, that's really straightforward. I'll run a vulnerability scanner. I'll count up all the vulnerabilities, and we'll watch them grow, and we'll watch them shrink as we remediate. That's metrics, and I'm done, right? And I'll apply that to everything."

Richard Seiersen: While I think that's great, that's a good start, I think there's more to it. Really if you look at the history of measurement and if you were really to talk to experts in the field, you would see that, engineers, scientists, they really retain their uncertainty in measurement because this is really important when it comes to security. The reality is, we're never really exactly clear how many vulnerabilities we have. It's not for a lack of scanning. It's not for a lack of trying. It's just the nature of the work that we do is it's full of uncertainty. I mean, there are vulnerabilities that are in our systems that have been there for days, weeks,
months, years, and many of them are being traded in the black market. We’re not aware of them, and eventually we will become aware.

Richard Seiersen: So, in what we’re doing, if we don’t account for some level of uncertainty in our measurement, we’re actually, perhaps in an unconsciously, incompetent way, we’re not telling the truth, right? I think that’s really, really key. So the concept of measurement is really about retaining your uncertainty. So that really means that we have to use methods that allow for that. There’s this massive amount of work and literature that goes back several hundreds of years on this whole process, so that really jumps to the methods and measurements.

Richard Seiersen: Then I’d say the object of measurement is really key. How do we know, what would I see occurring, that would let me know that this capability is improving? What actually is the empirical evidence that lets me know that the things that I bought, the people, process, technology, right, the things that I’m doing, are actually making things better? That’s the object of the measurement.

Richard Seiersen: I think oftentimes we don’t measure the right things. I don’t know if that sounds hokey or mystical, but it’s a common problem. In fact, in my talks I actually mention this a lot. I talk about the problems that there were in the actual ... There’s a problem in south Florida in the Everglades. They have problems with manatees. I talk about how they mismeasured that. Then I go into the topic of World War II and bombers and how they mismeasured. They used to look at the bombers that came back with holes, and they realized, "Oh my gosh, we probably need to start looking at the bombers that didn’t make it back. Look at where the holes are from bullets or whatnot on those and patch from that perspective."

Richard Seiersen: Lastly, I talk about Moneyball. The whole story in Moneyball is the wrong object of measurement in baseball. What they started to realize is what really makes wins. What really makes wins is just getting on base, any way, shape or form. They really realized also that people who are good at getting on base are highly underemployed. In fact, most of them are in the farm league. They realized that runs batted in was the wrong measurement. It didn’t correlate highly at all. Actually, it correlated highly with expensive baseball players but not to winning.

Richard Seiersen: So I really spend a lot of time in my talks and training on talking about look, let’s talk about what are the right objects of measurement. How do we know we’re really measuring the right things? Then we can talk about the methods that retain our uncertainty. I write on this stuff. I speak on this stuff, Brian, so you really hit my sweet spot. So I can babble along on it.

Brian Contos: No, I love the stories, from manatees to World War II bombers to Moneyball, and I like the analogy there. You hit a couple of really key terms there, things like evidence and being quantitative and not just qualitative and measuring the
right things and finding the value. I think that really resonates with people today.

Brian Contos: A lot of folks think about measurement, and sometimes it's, "I'm going to run a bunch of vulnerability scans. I'm going to do some patching and we're going to look at the gap between the two." I'm not saying vulnerability scanning and patching is bad or red teaming and professional services engagements for pen testing are bad. But what I find is that they don't necessarily result in defensive value as it relates to your actual defensive solutions, your endpoint, your network, your email, your cloud security tools, or your actual defenders that are using those.

Brian Contos: Then on the other side of it, your defenders generally don't have that offensive mindset, so they haven't necessarily optimized those solutions to address what the red team is doing. That's this whole notion of purple teaming, right? And trying to bring these two groups together so we can start judging the value of these offensive efforts, these scans, these pen tests, on their ability to actually improve defenses and then measure that improvement.

Brian Contos: So, I guess, again, it's to that term I used earlier, which is maturation. We're getting to the point now where we're treating security much more strategically. We're reporting at higher levels, and when you start doing those types of things, you'd better come with real evidence to support that, or you're not going to be in the big leagues, if you will.

Brian Contos: So, let's dive in. You mentioned you're in the process of writing a second book now. What's that one about?

Richard Seiersen: Again, this is with Wiley Publisher. It should happen probably latter half of 2019. The original title was called Prove It: Confronting Security With Data. I'm thinking of changing the ... Well, actually we are changing the name to The Metrics Manifesto. There will probably be a subtitle that goes with that as well.

Brian Contos: Oh, I love it. I love it. That's awesome. Not that the first title was bad, but this one's awesome.

Richard Seiersen: Yeah. So, my first book was really along the lines of do I have the right capabilities, right? So, it was really measurement at a strategic level. It was really measurement for large, rare, catastrophic risk. So very actuarial in nature, I suppose, applied to security. This one is going to be much more tactical, very much oriented toward metrics, but really embracing more of a scientific or pure engineering perspective on metrics. Really evidence driven but still with the concept of retaining our uncertainty in measurement and really looking at, again, how do I know that the capabilities I've invested in are actually helping me get the outcomes I actually want and really trying to, again, be really clear
about how we measure the risk, how we communicate it, and how do we actually know.

Brian Contos: Yeah. I love the simplicity of it just at a high level. Hey, I've got a bunch of stuff, and I just want to make sure I'm getting value out of that stuff; it's doing what I want. At that level it is simple. It just makes perfect sense. It's the reality of that that we know can be challenging.

Brian Contos: I want to kind of combine two things. Certainly, we've been talking a lot about metrics now. You spoke earlier about the need to really hire the right team and get the right people in there and not just be technology focused. What's it like being on your team, having a leader that is very much in that metrics mindset and understands the value of measurement?

Richard Seiersen: Having done this for a while but always been this way, I've always been this way, I think it does take a particular sort of person to report directly to me. I'm not the 90 billion served, the McDonald's analogy, kind of guy. I think it's because I have a point of view, and it's a pretty strong point of view, and it's an unabashed point of view. I find that either people love it or hate it, and that's okay.

Richard Seiersen: So if you're the type of leader who is maybe really trained as an engineer, a real engineer, right, and you've been experienced and you've done it and you're the type of person who's maybe worked in critical infrastructure, real risks. You've worked for companies where if things go wrong, the world knows about it, or you have maybe a scientific training, physicist or things like that, actually all those things as a background sweep, had a rigorous security background, you're an engineer, scientific background--those types of people tend to really resonate really well. And typically, leaders report well to someone like myself.

Richard Seiersen: If you're a new person to security, you just want to go out and day in and day out build and get things done, that's great. We probably would need to shield you from me with a leader. Because, I mean, I'm just really evidence driven. I just really want to know does this stuff work, and I'm going to ask hard questions. If you are in that mode of "I just want to be a builder, please leave me alone," you won't do well with me. You just won't because that's it.

Brian Contos: Yeah. Long gone are the days of assumption-based security. Long live the days of evidence-based security, right? Again, I love the way that the industry is going that direction. I think it's something that we absolutely needed to do. Well, Richard, you're a serial CISO. You've been in security for quite some time. You've written a book. You're in the process of writing another book. You've had some great success. What do you think it takes today to be a successful and effective CISO?
Richard Seiersen: Well, let me just say that I'm still trying to figure that out for myself, so I want to be humble. I've had success, and I've had, I guess you'd call it failure, and everything in between. I think that's the reality. But I suppose I'd say there's kind of three things that I think about when it comes to being, I suppose, a qualified CISO.

Richard Seiersen: First of all, call it 20 years plus or minus five, right? Just roughly, of experience, 20 years plus or minus five, in security, right? Pure security at work. This is my opinion. Part of that experience, if not the majority of it, should go back to this idea. I said critical infrastructure. But the companies that you're defending have real risk, meaning if a bad day happened, it's the kind of thing where if you stopped doing what you're doing, your company did because of the security thing, the world would know about it. Not just because it would go out on Twitter and what have you, but things would stop working.

Richard Seiersen: So, you've had some critical infrastructure or some sort of real responsibility, even upwards of life or death. If you really haven't protected stuff that really, really matters, I think it's hard to really call yourself a CISO. You might be a security leader who has a lot of great experience, but if you, again, haven't had to really defend something that really matters on a global scale, I don't know, it seems to me that that would be difficult.

Richard Seiersen: Lastly, and you can't get this last thing unless you've had those first two things, is a point of view, a point of view. I think it's a point of view that should be something that you have developed that is probably ... It may not be entirely unique to yourself, but it's something that just perhaps distinguishes you.

Richard Seiersen: Don't just go out and get a point of view because you want to have one. It's something that really matters, that makes a difference, and that you've actually gone out as a leader and you've been participating in developing the security narrative, right? You're a part of security history. You've done some sort of contribution, be it research or otherwise, however that manifests.

Richard Seiersen: I'm not just talking about going and doing a lot of talks, public talks, or just writing a paper here or there. But there is something that you are doing that really is making a contribution to the corpus of security knowledge. So a real CISO should really be on that path to all three of those things. This is my opinion, but I've been doing this for a while. I'm a little older and, again, like I said, I have had successes and failures, so take what I say, I suppose, with a grain of salt.
Richard Seiersen: But if you don't have those three things, and this probably is more to hiring managers. This is maybe a conversation for board members or CEOs. If you're looking to hire somebody and you're in critical infrastructure, financial services, ven tech, or again, some sort of other fieldwork, if you stop part of the world stops and they know ... If you are hiring a CISO and they don't have those three things, you've really got the wrong person. That's my opinion.

Brian Contos: Yeah. No, I appreciate you sharing that opinion, and I appreciate the fact that you had some specifics. It wasn't some very lofty sort of ethereal statements, right? That's predicated on your experience, and I'm sure some hard lessons learned and some bumps and bruises along the way to get there. So, no, I really appreciate that. So, do you feel security then is an engineering issue? Is it a business issue? Where do you fall on that question?

Richard Seiersen: So again, going back to the objects of measurement, the things that we choose to do from a strategic perspective must correlate to both business and risk drivers for the particular business and industry that you're in. I know that sounds lofty, but if you're going to be going to a board or to your E team or whomever, you really should be able to say, "Listen, we're choosing to do these things because of these business and risk drivers."

Richard Seiersen: When I say business drivers, oftentimes what that really translates to is someone who is kind of measurement oriented. Engineers and scientists, financial people are measurement oriented. I'd say serious people are measurement oriented.

Richard Seiersen: So, the business drivers really are what is the opportunity lost if we don't do this thing, right? What is the opportunity lost if you become a boat anchor as we try to do this thing, right? So, there are business drivers. We are going to go into a new market, or we're going to go into a new region, or we're going to go into a new region and new market and we have this new business strategy. Or, in fact, we are changing our business model. We're going to a ... Maybe you're going into a marketplace ecosystem, right?

Richard Seiersen: So, taking those things into consideration, that's going to really shape the types of choices you're going to make in people, by the way, and process technology. Then, of course, what are the risk drivers, right? Again, going back to the idea of critical infrastructure, are you protecting financial transactions. Are you working in pharma, and you're protecting IP? Are you in manufacturing, right? And again, IP and, of course, supply chain becomes really critical. So what are the risk drivers that are going to inform the choices that you make?

Richard Seiersen: So, it becomes both a business and, I'd say, engineering conversation. It really is both. You have to embrace both. Again, on the engineering side, I would actually argue ... When people say, "Oh, Rich, you seem to be really into
metrics," in my response to them, I'd say, "No, I seem to be really into security. What are you into?" Because if you are the kind of security person who is incredibly biased and says, "I think security is an engineering problem," and you are not driving what you do from a measurement perspective, you are not an engineer. You just aren't.

Richard Seiersen: By the way, I come from a poet's background, all right? I really do in terms of my education, well, my education in school. My education subsequently has probably been more in line with an engineer. If you had an engineer, you had an actuary, you had a scientist, and they looked at least at the way that I am purporting to view metrics, the way I'm looking to do both forecast but empirically measure the phenomenon, they would recognize it. We know that because our book is required reading for the actuarial exam or whatever. But they would recognize it. They would not see this as foreign.

Richard Seiersen: On the other hand, if they had looked at what someone else might consider to be engineering, they might say, "Well, I see you doing work. I see activity going on." But typically an engineer is someone who's going to shoot a rocket to the moon, someone who's going to build a bridge, someone who's going to do some sort of engineering activity. They would really be looking at what's the specification, right? What is the expectation? What is the output? What does it mean to scale from a measurement perspective?

Richard Seiersen: They would be looking at those things, and the designs would be targeting those outcomes. They wouldn't just going and "I'm going to go build a bridge." Build, build, build, build, build, build, build, build. Hope it works, right? No. They're going to be starting with okay, what is the expectation that we have here? That's engineering, and I'm going to tell you I don't see much, if any, of that happening in security.

Brian Contos: Yeah. I think that's well put. We've gotten accustomed unfortunately, I think, in security to looking at things backwards and upside down for so long that they start to look right. We think that the way we do it is the way we've always done it.

Brian Contos: You're absolutely right. You're not going to just go build 50 bridges and hope that the last one actually stands. You need some type of very process focused metrics to do that. Richard, as we wrap up here, and this is something I like to ask all of our guests, who is your favorite superhero or super villain and why?

Richard Seiersen: Oh my goodness gracious. Who is my favorite? I'm going to say Wolverine. The reason I say that is because he's got some killer muttonchops, and I've always wanted great muttonchops. One of my favorite security heroes, Dan Geer, has great muttonchops, so therefore that's my rationale.
Brian Contos: Dan does, in fact, have muttonchops. I never thought of that, but I'll never be able to think of Dan Geer the same way now because now he's a Canadian superhero with adamantium claws. Well, awesome. Well, thanks, Richard, and thanks to all of our listeners for joining. Be sure to check out other Security Effectiveness Podcasts sponsored by Verodin.