

BUDGETS, BUREAUCRACIES, AND BEHAVIORS

11/08/2018

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.

Brian Contos: I'm your host, Brian Contos, and we've got a really special guest today. Joining me is Malcolm Harkins. Welcome to the podcast, Malcolm.

Malcolm Harkins: Thanks, Brian. Happy to be here.

Brian Contos: Hey, Malcolm before we get going, could you give the audience a little bit of background on who you are and what you do?

Malcolm Harkins: Yeah, I'm Malcolm Harkins. I'm currently Chief Security and Trust Officer with Cylance Corporation. So, I manage all of our internal controls and security risk and compliance activities along with dabbling in corporate social responsibility and some of our ethical work internally.

Malcolm Harkins: Previous to that, spent 24 years almost with Intel Corporation, so a little bit of an oddball, worked for two companies in 27 years. My last job at Intel was Worldwide Chief Security and Privacy Officer, where I oversaw everything from corporate emergency management, all aspects of information risk and security, product security, not the features for sale, but the development processes and practices to try and minimize vulnerabilities in technology.

Brian Contos: Well, just a few hats in there, of course, in that 27 years of time, I'm sure. So, Malcolm let's dive into this, this juxtaposition of these very, very different companies and not just based on size, but what was it like leaving Intel after 24 years and joining Cylance? And when you joined, I'll just mention to our listeners, this wasn't the Cylance we all know and love today, this was a very early stage start-up. Just kind of getting out there and getting moving. You had left this behemoth of Intel to go to this relatively unknown [company]. That must have been an interesting journey.

Malcolm Harkins: It was. It was exhilarating, and I get asked this question a lot. To be honest, other than the size and complexity and stuff like that, it wasn't much of what I'd say substantial change for me. I mean, both companies are in the tech industry. My role, by and large, is very similar other than for a smaller company. But, I kind of have a core belief when you're choosing a company, manager, a job,

you've got two basic choices: you're either running away from something or you're running toward something.

Malcolm Harkins: If you're running away from something, it's only out of dumb luck, you end up in a destination and if you're running toward something, there's purpose, passion, curiosity, something that propels you. I ran at things for 24 years at Intel, and Cylance was the next thing I needed to run towards because of what Stuart McClure and Ryan Permech had created, why they had created it, what the product was capable of doing, and my core belief system in terms of what's been wrong with the industry and how to manage risk.

Malcolm Harkins: So, first rule of choosing a job and a company and a manager: run toward something. Then you always have to find three things when you get to an organization to really be in your ideal state. I think it's a leadership philosophy that I have, but it's also something that I seek for myself. I think people need to routinely be able to say to themselves six words: I believe, I belong, I matter. They need to believe in the mission, they need to believe in their management, they need to believe in themselves and their team. They need to feel like they belong, because frankly we all want to know that the organization we are a part of, people frankly give a shit about us, and then the work that you do and the work that your group and the organization does has to matter.

Malcolm Harkins: For me, because I've always thought that way. I've managed myself that way and tried to create that environment and culture for the teams that I've run. It wasn't that much of a transition, because I felt more strongly in Cylance that my belief structure and my ability to have an impact would be greater, and I think has been greater than anything I ever did at Intel.

Brian Contos: Yeah. You know, that's what I've always respected about you, Malcolm. You take a very personal, heartfelt approach to what you do, where you're doing it, who you're doing it with. It's not squarely based on hey this is awesome tech, and I think there could be a great upside here. There's a lot more to it, which I think makes you the leader you are today.

Brian Contos: But let's talk a little bit about the differences. What's the difference — and maybe there's no difference at all, I'm guessing maybe there's some — but what's the difference between running a small team at a smaller company versus the hundreds of employees that you used to have reporting up to you in a company with well over 100,000 employees?

Malcolm Harkins: Yeah. There is a significant amount of difference there. Because again, when you look at the span that I had and the governance and oversight that I had, there was several hundred folks, and cross-secting 100,000 employees. Email volume was high, because of the size of the organization, the size of the team

that I managed. Budget complexity was greater, because I had tens of millions of dollars I was responsible for [and] making decisions around.

Malcolm Harkins: That aspect of it, I've always said there's kind of two battlefields a CISO or a Chief Security Officer faces, the external one that we all talk about, and then the internal one of budgets, bureaucracies and behaviors. Let's just say in a large company, and with what I had to deal with, that internal battlefield was much more significant to go navigate and work through. That's a big difference that I don't have at Cylance.

Malcolm Harkins: The team dynamics of managing a small team is... I miss sometimes running a large organization because I liked being able to do that. But the ability to have one-to-one interaction is much greater with a small team, which I also really like, because it creates a stronger personal connection.

Malcolm Harkins: So, you've got those type of differences by and large, and then the fact that I've worked for somebody who can still deconstruct malicious code when the last time I wrote code was in Fortran in the 90s. There's dynamics like that, that are dramatically different than Intel, considering some of the folks that I've reported to, even though we were in a technical company, didn't have hands on technical competencies like the leaders at Cylance do. Like I said, a variety of different organizational dynamics, but by and large, the allocation of time is a little bit different. I spend the vast majority of my time external facing, and that's because we're a third-party provider to folks, so I have to engage with our customers on their assessment of us as a potential risk to them, explain the privacy dynamics, what we do from a compliance perspective, and then help drive the business and do public policy related stuff. At Intel, I spent maybe 5%, 10% of my time external facing. So that's also a big mix change of my time allocation.

Brian Contos: Wow, wow. I didn't realize there was that big of a difference. That does make sense. Let's take two of those Bs, budget and bureaucracy. When it comes to you and your team being more effective, do you find it more challenging dealing with a large bureaucracy where you have a much larger budget, as opposed to a lot less bureaucracy, more streamlined, smaller company, but maybe not the budget that you had before? Which paradigm leads to, at least in your experience, a CISO being able to be more effective?

Malcolm Harkins: It's a great question, and like I said, that is an internal battlefield. If I'd looked back in my early days, getting into security more out of accident in post 9/11 and Code Red and then when I was asked to go run security and business continuity in the IT organization, Doug Bush who was the CIO, he hired me because of my prior background in finance, procurement, project management, business operations. He knew I knew how the company ran, which was different than the technical security competencies of the small security team Intel had.

So, he knew I would win on that internal battlefield and learn from the security team, and they would learn from me.

Malcolm Harkins: So, in those early days, because I knew all those mechanisms and I knew how to win on that internal battlefield, it was actually for me, quite easy. But as Intel evolved, executives changed, their belief structure on what to do and how to do it versus mine differed. That became, in many ways, much more problematic and challenging. The budget bureaucracy dynamic shifted a lot come 2012, 2013 and going forward. And Cylance, it's pretty simple. I report to the CEO, he gets it. Our general counsel, the finance team get it. Again, the budget's smaller, but by and large, I can tell you with 100% certainty, having a smaller budget and a smaller team with people with the same mindset on what to do to actually best manage and mitigate the risk, my life is a lot easier. I'm not playing Whack-a-Mole with malicious code. I'm not getting woken up at two in the morning routinely because of an incident or an issue.

Malcolm Harkins: So having a culture of controls that puts you in a better spot to manage and mitigate risk makes that easier internally at Cylance than it was at Intel.

Brian Contos: Yeah. I always find it's great when a non-technical, non-security leader, business decision maker, whether it's a board or a CEO, clearly you have a very technical and security savvy CEO in Stuart, but others kind of get it. They're on board with always having to fight that battle.

Brian Contos: Let's go into a little bit of your leadership and management practices that you have. Have they fundamentally stayed the same, or did they have to morph sort of along the way, and as you grew in this new role?

Malcolm Harkins: You know, they've in essence stayed the same. When I was back at Intel, when I went from running kind of a smaller security team to larger organizations, one of Intel's CIOs had told me at one point my leadership style and approach would have to change for me to scale. I basically said, "I don't want to change. You're right, I'm going to have to deal with how I interact with people differently," because I make a lot of personal connections, and I like having that one-to-one relationship with folks. As I went from managing dozens to managing hundreds, that had to change a little bit, but I also did not hide away from any engagement or dialogue that any employee wanted to have with me.

Malcolm Harkins: That sometimes became a calendar challenge, but I've always kind of... there's a book called The Leadership Challenges that Kouzes and Posner wrote back at least 10 years ago or so. I used to teach The Leadership Challenge Workshops before. There's a quote in the book that I love, that "leadership is the art of motivating others to want to struggle for shared aspirations." That to me is one of the best definitions of leadership I've ever seen. I subscribe to that

philosophy, which is why that culture of “I believe, I belong, and I matter” is important to me.

Malcolm Harkins: Then it just becomes how you engage with people to deal with it. But by and large, I think my management style is the same both as it was at Intel as it is at Cylance, and I have some former Intel employees that were part of my team that are at Cylance, and they came because of that and because of Cylance. They've told me that I'm pretty much the same person, the same way. I think I'm relatively consistent, good or bad, from that perspective.

Brian Contos: Yeah. That's refreshing to hear, because often you'll find people that say, "Oh I could never work for a start-up or a smaller company. I'm just so accustomed to working in the large organization." While I think there sometimes is some truth to that, just in terms of the pace at which individual operate. If you're okay with that pace, the fundamentals don't necessarily change. You're a great example of someone that's been through that. And you've also done it with multiple titles. Let's kind of switch gears and talk about that a bit.

Brian Contos: What are the differences from your experience between being a CISO, a Chief Security and Privacy Officer, as well as a Chief Security and Trust Officer. How do these roles and titles differ?

Malcolm Harkins: It's interesting. I've always had the same picture of what I'll [call] "the Kaleidoscope of Risk." Whether I was the CISO, a Chief Security and Privacy Officer or a Chief Security and Trust Officer... so I've got a picture that I've put in my first and second book, I've used it in speeches, of all the dynamics of risk that have to be seen. I think though in the industry, CISO primarily means I report into IT, and my scope is IT and that's it. I always thought when I was CISO at Intel, that my scope was actually larger than the CIO's, regardless of whether or not I reported to them, because information risk in many ways was well outside the scope of what most CIOs had accountability for, because there were things in factories, there [were] other aspects of intellectual property that were tied in with business units. You had e-discovery issues. You had international traffic and arms regulations. You had export control.

Malcolm Harkins: There [were] a bunch of different dynamics to things, and other interdependencies with aspects of the business and other compliance things that I always thought as my role as CISO. Now, when I became Chief Security and Privacy Officer, that was when I also picked up more direct responsibility for product security at Intel, versus indirectly influencing it.

Malcolm Harkins: To be honest, the job title was going to be something like Chief Trust Officer, but Intel's Chief Technology Officer didn't want another CTO, so it became Chief Security and Privacy Officer. I had always had, from the early 2000s, the privacy team underneath me, that partnered with the legal team, who had the legal

privacy acumen to interpret the law and do stuff like that. Just like at Cylance, Chief Security and Trust Officer, like I said, by and large, my scope is about the same, and I dabble in a variety of things like ethics and compliance, much like I did at Intel. Corporate social responsibility, much like I did at Intel. But I have, at Cylance, a little bit of a smaller team, it's easier to do it rather than at Intel there was somebody in a whole group that owned social responsibility, that I kind of plugged into and worked with. There was a Chief Compliance Officer that reported in to legal that ran the ethics and compliance oversight committee that I was one of the senior managers steering that ship on.

Malcolm Harkins: So, like I said, the dynamics of how you govern that stuff are a little bit different, but by and large, for me, the governance structure that I've always tried to put my fingers into are the same, because I see security and privacy as a social responsibility. I see it as an ethical issue in addition to just the compliance and risk aspects of it. So, like I said, there's a lot of similarities, just the nuances of the structures are a bit different.

Brian Contos: Yeah, yeah. I love your statement, and sometimes it's just because the CTO doesn't want the same acronym.

Brian Contos: Malcolm, you mentioned a couple of your books. Why don't you give a quick little shout out the titles and what those are about real quick for everybody?

Malcolm Harkins: Yeah. So, I've got two editions of basically the same book out. Managing Information Risk and Security with my tagline, Protect to Enable, because I've long believed that the security teams' mission is protect to enable people, data and business. If you're not protecting to enable that, it's protection for protection's sake, which is a waste of time, a waste of money, which means you really have to understand the mission objective of the particular business unit or broader organization, and make sure that you are protecting to enable that mission and those business outcomes.

Malcolm Harkins: So, the second book was published about two years ago, it was August, September of 2016. First edition was in late 2012. Between the two of them, there's been over 200,000 downloads and probably 75,000 hard copy sales. You can get it from the publisher, Apress. If you like electronic books, both versions are available for free, both in Kindle as well as the other e-book versions on the publisher's site, or you can get it on Amazon if you want a hard copy.

Brian Contos: That's great. That's great, and congratulations on those numbers, those are fantastic.

Malcolm Harkins: Thank you.

- Brian Contos:** That term, protect to enable, I really think it resonates today as we see the maturation of our space, and nobody ever opens up, let's say a bank, for example, and says, "Boy, I'm going to open up this bank. It's going to be the most compliant and most secure bank in the world." That's not your business mission. So having security enabling that, I think is really where everyone who wants to go, whether or not they're moving there at the same pace is a different question. But, as we wrap things up here, Malcolm, and we like to ask this of all our guests. Who's your favorite superhero or super villain and why?
- Malcolm Harkins:** It's interesting you talk about heroes. I had been doing a quick video thing last week at our user conference, and one of the folks asked me for some closing comments, and some stuff just came out of my mouth. It was because I really see Cylance customers as heroes. They took a leap of faith with a start-up a few years ago, and changing the dynamic and really going with a prevention first control philosophy. They're seeing the benefits out of it, certainly fueling Cylance's growth.
- Malcolm Harkins:** The comment that I made is, "Heroes help us realize and see that hope is real." So for me, I'm a hopeful person and for me, my superhero is one that's driven by principle: it's Captain America. And I love the character because it's principles over politics. There's a focus on equality and justice. You have focus on honor and doing the right action. So, there's a moral compass so to speak, to that character that strongly resonates for me. So, Captain America is my favorite superhero.
- Brian Contos:** I love it. I love it. I think that's an awesome choice. And I love your perspective on the customers as well. I was in Texas earlier this week, meeting with a number of oil and gas companies. Some of them happen to be Cylance customers as well, and they mentioned the point in time when they said, "Well, there's this new company coming on board a few years ago, their name is Cylance, and they've got this really cool approach to end point, and we've already got this legacy control, and maybe we'll run the two together side by side." So many of them have talked about, "Yeah, we just run Cylance now, and we've just had so many issues with the other stuff, whether it's product A, B, or C." So I really think it's a kudos to Cylance and the team and the technology and the feedback from customers and how the product has evolved over the years to be sort of the powerhouse it is today.
- Brian Contos:** Malcolm, thanks so much for joining us on today's podcast, and thanks to our listeners for joining. Be sure to check out other versions of the Cybersecurity Effectiveness Podcast, sponsored by Verodin.