uberknowledge

Malcolm Harkins, CSO, Cylance

The Rise of the Cyber Industrial Complex

Malcolm declares the security industry is not to be trusted because it profits from insecurity.

00:23 Non-traditional beginnings to a CSO career.
02:02 The unusual role of a CSO in a vendor.
02:24 Security needs to crawl out from under IT because it touches every aspect of the business.
04:04 The security industry is not to be trusted because it has no economic incentive to solve the problem.
06:12 Business wants three main things: the risk managed, the cost lowered, and the friction controlled. CISOs need to be measured on that.
8:59 The rise of the cyber industrial complex: defense and depth has actually turned into expensive depth
11:19 The cybersecurity industry is not economically motivated to solve the problem. We need to demand attribution to the controls that failed and hold the industry accountable.
13:27 The role of security in M&A processes: build the cost of remediation into the acquisition budget and this should be bidirectional.
16:24 Selling on fear is like eating junk food: short-term satisfaction, long-term ruin.
17:36 Please don't ask me for my risk register.
20:21 If we focus on protecting our customers to the best of our ability, the result will be the limitation of liability.
23:36 We focus on the fact that technology done right can connect and enrich lives and can create social and economic benefit.

Ashwin Krishnan: [00:00:00] So with me on the UberKnowledge podcast, I have Malcolm Harkins from Cylance. Malcolm, you and I have known each other for a long time. So why don't you start by giving the audience a little bit of your background and where you are right now at Blackberry. But also, I want you to touch on something we just briefly talked about: your last blog on the rise of the cyber industrial complex and really what that means in the broader sense.

Malcolm Harkins: [00:00:23] Yeah. So, a little bit about my background, it's oddball relatively compared to most Chief Security Officers or Chief Information Security Officers. I'm not a technologist. I have an undergraduate in economics, an MBA in finance and accounting. The 24 years I spent at Intel, half of that was in different finance procurement business operations of startups, until I tripped my way into security after Code Red, Nimda, and 9/11 when Andy Grove was frankly beating the crap out of his corporate officers to deal with the availability risk issues. Since I had thick skin and wasn't afraid of him, Intel's CIO called me up and asked me to run security and business continuity for him. And you know along the next 12-13 years, I put my arms around every aspect of information risk and security controls compliance. I ran corporate emergency operations. I eventually became Intel's worldwide chief security and privacy officer overseeing all aspects of information risk, product security, and services and all that. Corporate emergency management, physical security matrix and then I had a bunch of all the other compliance aspects that touched technology as well. Then I joined Cylance about three-and-a-half years ago as a Chief Security and Trust Officer and basically have the same elements just in a much smaller company, but I also spend a lot of time doing public policy work, focusing on corporate social responsibility, and other ethical considerations around the use and application of technology.

Ashwin Krishnan: [00:02:02] Wow. OK, so first question: It's very rare that you actually have a Chief Security Officer in a vendor, right? And believe it or not, when I first saw that, I was thinking, "OK, is Malcolm really doing this in a vendor?" So, tell me a little bit about why this is important and why we're not seeing more of that in the vendor community.

Malcolm Harkins: [00:02:24] Yeah, well I think you do have it in a few of them. You know, Jon Stewart at Cisco used Chief Security and Trust Officers, a friend, well-skilled individual, and stuff like that. You've got it in a few spots. My view of information security in the CISO role, and I've written this in my book, it needs to evolve from just being buried under IT. It is related to IT, but in many ways the scope and purpose and breadth of it is different. I've created a Venn diagram, so to speak, that's little bubbles. Information security has a touch to IT, but it touches all other aspects of the business. It has aspects of privacy. And that's why I was chief security and privacy officer at Intel. Even though I had a legal counterpart interpreting the law, I had to have the risk and compliance and technologist codify that into the controls. There's the same thing with other legal compliance issues, you've got business continuity disaster recovery, you've got product security. The security around the development design and validation of the technology itself and they're interrelated risk issues, physical security is an interrelated risk issue. And so for me I've had a view, and I hold to this very strongly, I did it at Intel, I did it at Cylance, and I will at BlackBerry, that these are integrated risk issues that need to be at the C-suite level; you need to have a chief security and trust officer. And we need to do that in the vendor community because it is a trust problem. And I'll tell you what I tell everybody when I'm onstage, most people should not trust the security industry. The security industry profits from the insecurity of computing at an economic level. The industry has no economic incentive to solve the problem. That's why I left Intel. That's why I joined Cylance. That's why I see this as a trust problem.

Ashwin Krishnan: [00:04:23] So, you mentioned the word ethics and your definition of how a CISO's role starts everything from physical security to product development to testing to third party integration, that's a very atypical view. Is it the right view? Absolutely. I agree with you. But given the complexity of interpreting compliance regulations — GDPR, CCPA, I could go on and on — given the lack of cybersecurity skills, there is an argument to be made, a wrong argument, but an argument to be made that the CISO is already under the gun. He or she is constantly having to fight for budget with the CMO, with the CIO,

and others. How does somebody rise above the noise and be that forward-leaning, ethical and trustworthy evangelist that you have been all your life?

Malcolm Harkins: [00:05:22] You know it's funny. I literally just walked out of a coaching one-on-one with a Chief Information Security Officer for a company in Europe. They're relatively small. He was asking me how to transcend from being the hands-on person with a small team into the business strategist that keeps their fingers in all the tactical issues but is forward thinking and doing all these things. So I'd described that bubble chart. I think the way in which you do it, the way in which I've done it, is I look at it from the macro perspective around how these broad aspects of information risk affect a business, and I bind them to the mission of the business.

[00:06:12] Then from there look at it and ask what is it the board, what is it the CEO, what is it the shareholders want out of this broad security team? I've written about it and I call it my nine boxes of controls. We can articulate this stuff, but there's three primary business outcomes that the business wants. They want the risks managed. We see day in and day out that the risk has grown unchecked, unmitigated, and unmanaged. It's been growing exponentially. So, the C Suite wants a demonstrable and sustainable bend in the curve of risk to reduce the impact on the company, shareholders, and its customers. But they also want it done in a cost-effective manner. They also want and need a lowering and flattening of the total cost of controls because we're throwing money at the problem and haven't solved it. So you've got the worst business answer possible: my risk is growing unchecked, and I'm throwing a shitload of money at it, and I don't get a result. Now the other thing is controls are a drag coefficient. They slow down people, data, and business. They impede business velocity. So, they also want a control philosophy and control paradigm that reduces that friction on the business velocity. So, three macro things: risk, cost — and cost meaning total cost, not the budget of the security officer, the total cost to the business — and friction control. If you walk in and say, "I am going to be measured and accountable on three macro metrics: risk, total cost, and control friction. Here's where we're at today with that. Here's the investment and

resources I need. And here is how I'm going to turn all three dials to reduce risk, lower and flatten cost, and get out of the way of the business velocity." What CEO, business unit general manager, or board would not invest in you?

Ashwin Krishnan: [00:08:20] That's a great question. And I haven't heard it articulated that way. So, again I go back to the blog that you referenced before we started recording on the rise of the cyber industrial complex. Again, in this theme of the CISO and his or her view of the world and the transcending that they need, how does the cyber industrial complex affect the thinking? And in those three frameworks you've talked about, risk, cost, and drag coefficient. Does that translate one-on-one into the cyber industrial complex or does it need more controls?

Malcolm Harkins: [00:08:59] Well what's happened, and what I reflected on as I was getting ready to do my talk yesterday at RSA, was what I called expense and depth because the notion of defense and depth has actually turned into expensive depth, meaning we have this burgeoning cost. And as I said, the security industry profits from the insecurity of computing. So, if I'm spending more money and still have risk, the industry continues to grow and likes its growth, so therefore you get the rise of the cyber industrial complex.

[00:09:30] Go back 17 years ago, my first RSA, there were a couple hundred vendors, a few thousand people. In 2010 I won the RSA Conference Award for excellence in the field of security. I received my award in front of 7,000 people. What do we have here today? 45,000 people, several hundred vendors, and probably thousands of other vendors walking around the streets all purporting to sell solutions to manage the risk. But that's been happening for decades now, and the risk has grown unchecked and unmitigated.

[00:10:01] When Eisenhower did his famous military industrial complex speech the day before he left the presidency, he talked about the defense industry and how in previous presidencies and up until World War II the defense industry came in to be when we needed the armaments. But then because of the world

change we needed a continued defense industry. And what he worried about, which you can argue may have come true in the military sense but certainly has come true in the cyber sense, is that the profit motives of that industrial complex take a hold of the public policy. They take a hold of the perspective. They're marketing for their own profits.

[00:10:43] In the cyber industry you can see this manifest itself in the fact that we haven't dealt with the risk. We've spent more money. But the other thing from a public policy perspective is, what are the security industry trying to do? They deflect accountability. Every time somebody has a breach, they say an advanced adversary. Well it's not that advanced to get somebody to click on something sitting on their box because of the shitty controls that are in the environment. So why do we call that advanced? The cybersecurity industry also, instead of focusing on the real root cause of the problem, focuses on who did it.

[00:11:19] Now, a law enforcement nation state needs to know attribution for that, but as a CISO, I can't control the threat actor and threat agent. What we need, and what I said at the Federal Trade Commission back in December when I gave testimony, is public attribution to the controls that failed. We need to know what technology, what process didn't work. If we do attribution to the controls that failed, then we can learn, and guess what? Instead of the stocks booming for the cybersecurity industry after WannaCry and all those other ransomware issues, the companies who didn't protect their customers, their stocks should have plummeted, and they didn't. And so, we have perverse economic incentives that the industry is feeding, they're marketing and they're deflecting accountability. And what we need to do, and what I put in my talk and what I put in my paper, is we need to stand up as Chief Information Security Officers and Chief Security Officers and demand the attribution to the controls that failed and hold the industry accountable for what they've not delivered on.

Ashwin Krishnan: [00:12:32] So this gets into the next question: learning from past breaches. Marriott is obviously top of mind. Talking about deflection, so you

bought Starwood, M&A cybersecurity risk assessment was not in the play book, or if it was, it was probably a footnote.

[00:12:52] Now as a CISO in your CISO community, is there talk about how we learn from what's happened out there? And, like you said, you have three control frameworks. If M&A is going to be a big risk, are we doing the right sorts of things when it comes to acquiring companies? So the point is, like you're saying, the industry is certainly not doing itself any service from a vendor perspective, but from a CISO perspective is there also an eagerness and a willingness to learn and adapt?

Malcolm Harkins: [00:13:27] Yeah, I think there is, and I've had a lot of conversations with peers on this stuff. Certainly, in my Intel days there was a substantial amount of M&A activity and divestitures, and my security team, the privacy team, and the other compliance aspects of this stuff were plugged into the mergers and acquisition process. Not necessarily that it would stop a deal from occurring because if you're acquiring a company for scale, scope, intellectual property and stuff like that, if that made business sense, understanding the information risk issues wouldn't stop the deal.

[00:14:04] But what it can do and what I've talked to peers about is doing that due diligence instead of dealing with it after the acquisition closes. If you have an understanding of where they may have a compromise, where they may have a breach, where they may have lacking set of internal controls, can the finance guy in me add into the deal capitalization the cost of remediation?

Ashwin Krishnan: [00:14:28] Yep, that's a good point.

Malcolm Harkins: [00:14:28] Because you're not going to get the budget after the deal is closed. You've got to build the budget into the deal process. I don't know on the Marriott side what they did or what they didn't do, I'm assuming they did some level of due diligence. But the other thing I will tell you is, it's not just about who you acquire. You also have to think about who's acquiring you.

So as chief security and trust officer for Cylance, I mean we certainly just got acquired, but I also have to look at it and say, "It doesn't matter to me that you spent the money. I need to understand your state of internal controls in order to mitigate any potential risk or exposure to my company." My view on this is, it needs to be bidirectional. It doesn't matter if you're being acquired or you're the acquirer, you need a level of mutual understanding of the risks on both sides and mutual mitigation if necessary before you start connecting up systems and processes.

Ashwin Krishnan: [00:15:34] So I'm referencing back to a tweet from a Time article, which I found really refreshing, five things that tech leaders fear the most. You had called out Susan Liautaud, lecturer on ethics at Stanford University and ethics consultant, who said, "Think first, act second." That is completely the opposite if you go to the RSA show floor. Where it's all about, how do I get ahead of the competition, how do I get my next funding round. So again, having been on both sides, how does taking pause and, like you said, going back and figuring out what really happened, what controls failed us, what has to get deprecated versus how do I quickly use this breach as a mechanism to get more budget to buy more gear, I mean, how does it change?

Malcolm Harkins: [00:16:24] You know it's an interesting thing. I have this view, I actually wrote about it in my second book. I've done this, and I will probably continue to do it. When there's an incident I will leverage that to move the needle, but in essence, the equivalent to internal selling on fear is like eating junk food. It might get you short-term sustenance, but long term it's not good for your health because you get addicted to that, then you're always in a hurry and you're always reactive. Tactically you might need to do that, but there's a different strategic element to it. In fact, in a dialogue I was having earlier this morning with a company who has instrumented to do what is a very, very sophisticated pulling of data from different systems to do risk calculations to give you visibility in real time to risk. And I said, "Okay this is cool, but there's a difference between calculating risk and contemplating risk." And what I worry about is the overfocus on calculating risk.

[00:17:36] What kills me is when a CIO or somebody asks for your risk register. Ugh. OK. This is a path to mediocrity, it's like a CMMI model, right. Nobody ever strives for five because they perceive it to be too expensive. When you when you start getting into the overfocus on the calculations, you end up watering down and everything ends up in this green and yellow, in which case everybody says OK that's good enough. Right? Rather than saying, "Beyond the impact to the business, what's the impact to the customer? What's the potential societal risk?" I think we've got to frame this stuff with a mentality — we'll never achieve it — but we have to have a zero-defect mentality and we have to constantly strive for that instead of just saying well it's acceptable business risk. And I've had these arguments with folks, accepting risk and acceptable risk are two different things, and people confuse them. They think that accepting risk is a control. It's not.

Ashwin Krishnan: [00:18:49] Great. So, in one of your many articles you said managing information risk isn't about saying no, it's about protecting to enable people, data, and business. You start with people and data. Going back to the expanded view of the CISO, where it's not just about protecting the assets of the organization but the assets of who your customers are and their data. And I'm happy to hear the word trust being used liberally here at RSA. But when, pardon my French, the shit hits the fan, are you going to do the right thing? Are you going to talk about breaches that have happened? Equifax is a great example. They dragged their feet, dragged their feet, dragged their feet. So, is there a cultural shift of saying, yes, we need to be worried about shareholder loss, we need to worry about regulatory noncompliance. But at the end of the day, like you said, if you start with people, if that's the first mindset that you have, is that the panacea where you start seeing changes?

Malcolm Harkins: [00:19:51] I do think there's a paradigm shift that needs to occur. I was in Australia about a year ago and did a Chatham House Rules dialogue and had some CEOs, some CTOs, some chief security officers, and some government folks. And as I made my statements of the security industry

profiting from the unsecured computing and you shouldn't trust them and all that stuff, a politician asked me, "How do you define your role as a Chief Information Officer or Chief Security Officer?" And I replied, "I'm a choice architect."

[00:20:21] I'm architecting choices for the business. Some of those choices I get to make, some of them a business unit GM gets to make, some of them the CIO gets to make, some of them the board has to make. But I architect choices in three ways: What's the risk to the business; What's the risk to the customer; What is the potential societal risk that's occurring? People say, "Yeah, but our focus is the shareholders and and we've got a focus on the shareholders," and I reply, "Right and I get that. I'm a former finance guy and I totally believe it." Let's go back in time when Ford developed and shipped the Pinto for seven years and Lee Iacocca was running the Pinto division. I don't think he was trying to kill people. But because they framed the risk in risk to the balance sheet and risk to the company, they risked their customers. We are doing that in the technology space today.

[00:21:18] It's not only in some cases the tech sector, but all the companies that are deploying and using technology. I've had massive arguments with peers on this. We've talked and gotten together for meetings to try to do a Hippocratic oath, a duty of care type thing. I blew up a meeting on this a few years ago. One of them came in after a big retail breach and they had just cleaned it up. I said, “We've got to figure out what outcome we're looking for.”

[00:21:46] And they were like, “I've got this because my CEO, my board told me to come in here with this, and this is the outcome we need to shoot for. What we've got to do is have a standard of care that limits our liability.” And I said, “That's exactly what Ford did when it shipped the Pinto. What did it do? It killed people because of the framing of risk — and it actually increased corporate liability”. I said, “That is an output. Now what we've got to do is frame the real outcome we want.” If we focus on protecting our customers to the best of our ability, the result will be the limitation of liability. But if you focus on limiting your

liability, you're going to throw your customer under the bus. The security industry has been doing that, the tech industry has been doing it, and I think a lot of the organizations out there today are doing it. Which is why it's a trust issue, which is a function of two things: competence and character. Competency is are we doing a good job and again the security industry hasn't demonstrated that. And then character, what's the intent and what's the integrity. Am I focused on the person I'm serving to get the result and outcome that they want? Which is why we should protect to enable people first, the data second, and then the result will be you'll be protecting to enable the business.

Ashwin Krishnan: [00:23:06] Very refreshing to hear that. Given that we are at the penultimate day of RSA 2019, what in your mind would be success?

Malcolm Harkins: [00:23:15] You know success for me, I'm a hopeful guy. The talk that I did the other day I used Greek mythology and I talked about Pandora, who was created by Zeus when Prometheus stole fire and gave it to the humans and then created Pandora with their jar unleashed...

Ashwin Krishnan: Not the streaming service?

Malcolm Harkins: [00:23:32] Yeah, exactly. Now you could argue Pandora's Box has been opened.

Ashwin Krishnan: [00:23:36] Right.

[00:23:36] And we haven't controlled it. But in Greek mythology there's another lesser-known Greek God, Elpis. This is the Greek personification of hope. And Elpis was, when the jar got opened, locked in the jar and so hope was never able to be unleashed and change the world and change the paradigm. My view of success is we deliver hope in terms of the future. We focus on the fact that technology done right can connect and enrich lives and can create social and economic benefit. My view of success is we treat information security as an economic inefficiency. It doesn't add to the bottom line of any organization in

terms of revenue or net income. The only bottom line it adds to is the growth of the cybersecurity industry. And we need to treat it as an economic inefficiency and get it to do what we need it to do, which is to prevent the risks at the lowest cost, get out of the friction that it's creating, and improve the business philosophy.

[00:24:47] So it goes back to those three metrics, right? Success is how do I lower risk, how do I lower cost, and how do I reduce control friction. And luckily, I can say with full testimony and testament, I've been able to do that since I left Intel and came to Cylance because I had a green field. I had technology that allowed me to do it. I had a philosophy that I had long believed in, and I had a management team who unleashed me to go do that and deliver that internally for Cylance and then go promote that view outside.

Ashwin Krishnan: [00:25:18] Yeah, I completely agree with you. I think what you're doing from a practitioner's perspective but also looks like impacting legislation and making sure that people who are creating laws are aware of what they're doing. But most importantly, just like you said, changing the lens to start with people, data, and finally the outcome is protecting the business in general. Thank you for your time, Malcolm. Always good to chat with you.

[00:25:43] Thanks Ashwin.