Title: Becoming a CISO: Formal and Informal Requirements
Transcript

Lisa Young: Welcome to CERT's Podcast Series, Security for Business Leaders. The CERT division is part of the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org. Show notes for today's conversation are available at the podcast website.

Hi everyone, my name is Lisa Young. I'm a senior engineer at CERT working on operational resilience. I'm pleased to welcome Darrell Keeling, Vice President of Information Security and HIPAA Security Officer at Parkview Health. Darrell is a graduate of the Chief Information Security Officer Executive Education program at the Heinz School at Carnegie Mellon.

This is the first podcast in a series that will talk about the role of a CISO in an organization and both the formal education programs available to aspiring CISOs, and the informal skills and education that a CISO needs to be successful.

So, welcome to the podcast series, Darrell. Thank you for being here.

Darrell Keeling: Thank you for having me.

Lisa Young: All right, so let's jump in and tell our listeners what all a CISO is and how did CISOs first come on the scene in organizations?

Darrell Keeling: CISOs came on the scene early on. They weren't named CISOs, or chief information security officers. They're really network technology professionals and things that really had an additive job function to look at security, and not in a huge broad scale. There was patch management and things of that nature, really common operational things that were being done to ensure that we had service uptime and things on our systems.

It wasn't until later when more incidents, and breaches, and data loss started happening that CISOs really started coming to the forefront and really providing, and helping chief information security officers and legal professionals with the specific information about how to better protect their organization. And a lot of that came along when emails started becoming available to the outside world in a sense of a person could get their email from outside their organization, where traditionally the only way they could get an email and things was inside.

There were websites and things of that nature that need to be protected as well as e-commerce and things started hitting the scene after we got out of the-- when bandwidth and things started getting more prevalent in things out there that we could have better response time on browsers and stuff. And as the CISO came forward, really what was happening, what was being asked of the CISO was really about how can we better protect, more specific information about laws that were changing, how to prevent breaches, things of that nature.

Lisa Young: So, then thinking about the companies that you know and I know, should every company have a CISO or an equivalent position?

Darrell Keeling: Yes, I believe so. I believe every organization, whether small or large, should have someone that is designated as a security professional, or a data security type czar that can really help the organization better understand what the risks are as they bring in different

new technologies as they go to the cloud, as they look at taking on data acquisitions and divestures kind of things.

They really need someone outside looking at what the security, and risks ramifications are for the actions in which they're taking and to really help their peers in networking, and their leaders in better understanding that risk and the costs for the direction in which they may go. So, yes, I do believe that they do need someone in that role.

The larger ones, yes they should have a designated chief information security officer. But some of the smaller ones could really have someone that's not a chief information security officer, but really designated as a security person, as a go-to person that can step back and look at things in more holistic manner and help provide business direction and things for their leaders.

Lisa Young: That's a good point you bring up. It seems like the CISO, or the dedicated security person that you described, would need to have both a strong technical acumen, but they also need to understand what the business drivers are. Has that been your experience?

Darrell Keeling: Yes, I feel that an individual that comes up through the technical track, that has a desire to really get closer to the business in kind of a business analyst type function, and has that business acumen or desire to learn their business from inside and out, outside of technical, they can speak techno, can gain the respect of their peers in the technical area, but also have that balanced respect from the leaders that are leading the business, and be able to translate technical speak to business speak to business speak, and in the reverse order just as much.

And as we get into more innovative solutions and things, and more people get exposed to the different applications and things that are out there, this becomes even more important to be able to translate the risk that we're seeing into business speak and vice versa so that the technical people can also understand why the business is asking the questions. And then the business can understand why-- or the technical people can-- or excuse me, while the business-- to help them understand the technical aspects.

Lisa Young: Yes, and I like that, that technology translation of the geek-speak to business acumen and business concerns. I think that's really important. So, then I said in our introduction that you're a graduate of the Heinz School program, the CISO program.

When you considered that program, were there other educational options that you looked at? And what made you think about formal education in your role as a CISO?

Darrell Keeling: Yes, so I personally came up through the technical track and had some really good opportunities in working with the business and had started really advocating to become a security professional early on in the days when email started becoming available for outside of things. And as I was progressing, there really wasn't a whole lot out there to really help a technical person make that transition to the business in the sense to be able to speak to leaders and translate technical speak to business speak.

So, there's books out there to help you gain soft skills and things to kind of help you understand that. They were more across all the different verticals of industries and things, really to help you develop as an individual and as a professional. So, you used a lot of those in the years past. And then there became some programs that were really short, short kind of programs that were a week-long that you go and you met with some of your peers in the industry.

You might be in a room with a senior leader of security and an analyst. But there really wasn't any that were purely security senior leaders, up and coming directors and VPs driving you learn more about information security, how to better explain things to their executives, how to really help elevate the chief information security role inside of an industry and really allow it to have the seat at the table, if you will, regardless if it's the executive table, or just having more of an authoritative opportunity in a room to speak about the risk.

So, as I was looking, I was looking for programs that were more structured around being a little bit longer, having deliverables in them that really resonated to what I was seeing that was things that the executive leadership and the boards were asking. And so, that's where I kind of fell into looking, and researching, and found Carnegie Mellon University and their six-month long program.

I had looked at other universities. And they had some up and coming programs. But again, they were one-week long. They really were almost similar to if you'd gone to a conference, and met people at a conference, and heard speakers at a conference.

Lisa Young: Right.

Darrell Keeling: So, really I was looking for something that was more in-depth, more around the kind of an academic that had a name to it that I felt that I could really help and be part of, that would kind of become hopefully the de facto standard. And I would be a person involved in that with a very strong peer group.

Lisa Young: Then let's talk about the formal programs, and specifically the Heinz program. Can you tell our listeners sort of how the program is structured?

You mentioned deliverables, you mentioned accountability, and you mentioned networking with senior leaders. But let's talk about the structure and the variety of instructors. And let's go down that path. And then we'll talk about the deliverable piece.

Darrell Keeling: Carnegie Mellon, the program is structured over a six-month long period. You go on site two times, one time in the beginning, one time at the end. And based on the groups that are there, there may be an optional opportunity to come in the middle as well. And in this program, you're being matched up with highly skilled professors that have been in the industry.

You're aligned with coaches that are acting professionals in the industry, and living the day-in life of a chief information security officer, chief risk officer, and really getting the opportunity to mirror up with them and learn and be mentored by that group of individuals, and then be structured in small teams of four to five to really work together and take all your backgrounds and work on a practicum, which is associated around an incident that has happened, and really kind of structure it based on the curriculum of the program.

It's a 13-module program that ranges everywhere from security structure and operations all the way through incident response, really evaluating laws, building threat programs, managing compliance, looking at how to look at return on investments and the different things you need to understand to build a case to sell to senior leadership at the end of the program, in front of a board, a mock board, to sell in front of, to really get their buy-in.

But you truly understand all the different disciplines within the chief information security role, to be able to sell them too, let them understand why would they need to invest several millions of dollars, or thousands of dollars to mitigate a risk that you truly are looking at the overall risk,

and looking at the company's revenue, how an incident, maybe a previous incident had disrupted the shareholders and stock. They're really taking a holistic view as you do as an executive of how things actually function inside of an organization.

Lisa Young: I like that structure. So, then talk about-- will you tell our listeners then-- so, what I heard was it's a virtual program. It goes together in a cohort for six months. The students are then further broken in to teams of four or five where they work on a practical problem. And at the end, they present those results through all the things they've learned over the curriculum to a mock board. I like the idea of the virtual program.

I also like the idea of cohorts and teams because you can learn from your partners. Will you talk about your role as a coach? I know once you graduated from the program you came back. And you've been gracious enough to give us your time as a real-world professional. Can you say a little bit about that and what made you want to work with the teams?

Darrell Keeling: I've been a coach for two or three cohorts now, an absolutely great experience working with the level of professionals that the Carnegie Mellon program pulls in. Everywhere from in the finance industry to the government, the FBI, the Secret Service, to retail, every vertical discipline that's within information security, there's been someone within my teams that I've coached that have brought that background.

And being a coach watching a diverse group of professionals with different backgrounds in similar but yet different verticals in what we do, in watching them really work on a problem, and you being able to coach them on the specific things that a security professional, chief information security officer executive really needs to understand as they're building out a case to sell it to a board of executives that may or may not have the background to really understand the technical or risk in which you're presenting and wanting funding for.

So, it's a really great journey watching the professionals that are senior, and watching them really learn as they go through the program, and really become more knowledgeable in why things are being asked, and better ways to present. And not only do you learn from the-- not only do the students learn from the coaches, the coaches are learning from the students as well. It's a really give and take. And then you put in the professors in there as well from the academic perspective and all the different areas that they get to see every day working with different businesses and things within the university.

You bring that together, and it's really a great opportunity in learning. And I just absolutely enjoy it. And I've got to meet people from all over the world that have gone through this program, Dubai, Brazil, several of the states. You don't ever know who's going to be in your class or be in your cohort. And just getting that international component to it, really makes for a great opportunity for a chief information security officer to learn.

Lisa Young: That's great. That's a great description. And I'm happy you're part of the program.

So, then let's step back for a second and say if one of our listeners is looking for CISO program, formal education, can you talk about some of the topics that should be covered, like what were some of the-- sort of the ones that you were surprised, or ones that you-- that are in the curriculum that maybe people don't think of?

Darrell Keeling: A lot of times, people looking at security, especially the chief information security officers up and coming, they're coming from the technical side. Then you have the ones that are coming from the business side. Really, you've got to have a balance of

information shared within this curriculum to bring a senior leader up from the business up to speed, to have the opportunity to be a chief information security officer. They've been in the business of many years in a lot of cases because this program really draws senior people that are acting already in these roles or aspiring to get to these roles.

So, the areas that I find really fascinating are building the insider threat programs. Or it's very fascinating to listen to the different industries and the behaviors and the differences between the government verticals and the retail and the healthcare verticals, really hearing that conversation and people collaborating on to better understand the material, but also understand the differences and similarities with an incident response threat program to protect an organization.

The other ones are around the information security laws. Carnegie Mellon brings forth some really good instructors, outside speakers there to talk about the different security laws and kind of some of the recent breaches and things and some of the different class-action lawsuits that have been out there and really kind of picking them apart, talking about them, and what does it mean from a liability perspective to your organization.

And this is a really good opportunity for professionals to hear that information to be able to take that and really be able to understand how they can translate the information to their specific board to get the board to better understand the reasons why we're spending money or doing certain things and to better protect the organization.

The other one is around governance, governance and information frameworks, talking about all the different frameworks that are out there, the NIST, the COBIT, the ISOs, and really talking about them and how they're structured to really bring value to your organization to enable you to be able to measure risk consistently and to be able to create a story behind all the investments that your board has invested in for security technology, but measure that, and then have something to tell a story back to them of how it's protecting their organization and how you're consistently lowering risk.

What I've seen in that one, that particular one there around the frameworks and governance and things, is that many professionals out there, chief information security officers, are going after funding. We know what the new technologies are. We know what they do. And that's wonderful. They mitigate risk and things.

It's the six months or a year later, where we've got to be able to tell a story to the board and things of how those things, those continual investments, are helping the organization to be able to tell that story. They gave them money. Now, they want to better understand the story behind how they are still protecting the organization because those are continual investments. And within the Carnegie Mellon program, or the 13 modules, you really start building that understanding of how to explain to that to your executives.

Lisa Young: And that makes a lot of sense, too because executives, as we educate them, become smarter about what we do. And they start asking the tough questions about why am I spending money to build a certain capability or buy a certain cost tool rather than outsourcing it, or rather than what are the structures that best fit what I'm trying to do strategically. So, that's an important topic.

Okay, well then, so is there anything that you would like our listeners to know about the program or your experience in the program? Or how can our listeners learn more about the CISO program at the Heinz school?

Darrell Keeling: The program is a very top notch program. It has over a hundred alumni now of very highly trained professionals in the industry. They're acting in the security, the governance, compliance type areas for the government, for healthcare, for retail, and every other vertical in between. And it's a really great opportunity in the six-month long program that it enables you to really build relationships with these individuals and things and really work together collaboratively in class, virtually, and really learn from one another. And these relationships extend beyond the six-month program.

Speaking for myself, I keep up with many of the cohorts just to see where they're at and where they're going and look and see how the program's helped them and how they're moving jobs throughout the industry and elevating themselves by having the-- taking the time and the investment to really build the understanding how to be a successful chief information security officer.

And with the different social media platforms out there, you can really see how people are moving around and elevating themselves to leverage what the program has offered them and from learning. And then I have several people that are in the cohorts that I've coached that come back to me and ask me, "Hey, have you ever seen this?" I reach out to other ones, as well.

So, it's really building relationships. And it's really become a really kind of a family, if you will, of security professionals that trust one another because they've gone through a six-month program which builds that rapport. And it's really helpful to have that. It's nothing better than having a sounding board outside your organization in order to really bounce ideas off of, not top secret information, not proprietary type information, just a lot of hypothetical thought process things that you really need to bounce things off of.

Have you see this in this way? Are you using the different new cloud platforms? And it really gives that extended opportunity out there when you're within this program to build those relationships.

Lisa Young: Sure because as you think about a CISO, I mean really protecting information and crown jewels of an organization is not for the faint of heart. And anything we can do to professionalize how that gets done and to share some of the stories so that we can all be successful I think raises the bar for all of us as professionals.

So, thank you, Darrell. I really appreciate it. Thank you for being here. And for our listeners, there will be some links and in the show notes that you can find out more about the program and more about the attributes that Darryl has talked about.

Darryl, thank you so much for being here today.

Darrell Keeling: Thank you for having me.