The Evolving Role of the Chief Risk Officer

featuring Summer Fowler and Ari Lightman as Interviewed by Will Hayes

----

Will Hayes: Welcome to the SEI's Podcast Series a production of Carnegie-Mellon University Software Engineering Institute. The SEI is a federally funded research and development center funded by the United States Department of Defense and housed on the campus of Carnegie-Mellon University. A transcript of today's podcast is posted on the SEI website at sei.cmu.edu/podcasts.

My name is Will Hayes. I am a principal engineer here at the Software Engineering Institute. Today I am pleased to introduce two of my colleagues from Carnegie-Mellon, Summer Fowler is a technical director of Risk and Resilience in the SEI's CERT Division, and Ari Lightman is a professor at Carnegie Mellon University's Heinz College of Information Systems and Public Policy.

Summer and Ari are here to talk about evolving role of the chief risk officer and a program that they work on together here at Carnegie Mellon. Welcome, Summer and Ari.

Ari Lightman: Thanks.

Summer Fowler: Hello, thanks for having us.

Will: Before we get started, could you tell us a little bit about your background, where you came from before you joined us and what your specialization is.

Summer: Great, thanks, Will, as you said my name is Summer Fowler, I've been here at the SEI for a little over 10 years. I started on the software side, and I made a switch over after two years into the CERT Division where we focus on cybersecurity. I am a technical director, leading a group of about 50 engineers. We are focused in three main areas: enterprise risk management which really ties in well with the program we are here to talk about today; the insider threat problem, and we are trying to solve that through tools, techniques and a lot of analysis; and then critical infrastructure protection via some technical and some capability assessments.

Will: Great. Ari tell us about you.

Ari: My background is sort of non-traditional academic: four startups, venture capital, and management consulting. I have been at the Heinz College since 2010. I teach a variety of classes at the intersection of marketing and IT. Classes I teach include Digital Transformation, Digital Marketing, and Measuring Social Analytics. I am also co-director of our CISO Executive Education Program, which is a joint program between the Heinz College and the Software Engineering Institute, and I am also a commercialization adviser with our Center for Machine Learning and Health.

Will: Ok, great, so you have really got a strong connection to industry and to what is happening in business, and you are also with us on Carnegie-Mellon's campus. You have got a fairly broad scope of responsibility, but we are going to narrow the focus of our conversation today.

So, we would like to start with conversation of what a chief risk officer is. Could I ask you to elaborate on that?

Ari: Chief risk officer is a relatively new role within an organization. I think it really got started with the understanding that risk permeates across the entire organization. All departments are dealing with different types of risk whether it might be cybersecurity risk, tactical risk, market risk, and those sorts of things. Coming together on a comprehensive enterprise risk strategy was necessary. That rolls up into an individual that could actually report to the board.

Summer: Yes, and Ari is right. What we are really seeing is that corporations are realizing that they have this wide swath of risks, and as Ari noted, they are coming out of these operational units. We are talking about all the things that he listed: reputational risk, the financial risk, that organizations are facing and having someone that is really that point person, that is looking across the entire enterprise and saying, *In order for us to achieve our strategic goals that the board has set out for us, these are the things that we really need to focus on in terms of how do we manage those*? *How do we position the risks that we face*? The chief risk officer is in that position to do [that].

Will: It sounds like without a focal point, we might be sub-optimizing on one topic or another when in fact, actions we take to manage risks and that topic really relate to another topic as well. So, this is a kind of a technical challenge that our person in this role would have. What other challenges would a chief risk officer really need to do well in conquering?

Ari: Well, I could start us off in saying that communication is critical. Risk is a multi-nuanced, multi-faceted, multi-tenant thing across an entire organization. So, being able to describe what the risks are without giving everybody the sky-is-falling scenario is really critical. So, what is the business value that gets imparted to the different organizations, associated with understanding holistic risk.

Will: Whereas one player at the table might view this thing in front of them as the worst thing they have ever encountered, but the person sitting next to them has two or three more that, on an objective level, they are much worse. It’s just that this thing, for this person, is the worst they’ve ever encountered.

Ari: Absolutely. We see breach attempts occur all the time, from an information security perspective. The CISO and maybe the CIO and the CTO, are very concerned around that very specific aspect. What the risk officer really has to understand is *what is the brand impact?* What is the reputational impact associated with some of these events occurring and the need associated with the data that their collecting? Those sorts of things.

Summer: The chief risk officer is really taking what the board and the executive management is laying out as goals for the organization, whether that is market share or it is reaching out and achieving some sort of goal that has been established by that board. The chief risk officer has to translate that down for the business units to be able to execute towards that goal.

Consequently, on the flipside, the chief risk officer is also then looking across the operations, measuring what is happening, monitoring what is going on, and reporting back up to the board or to executive management: *These are the risks that we’re seeing. Here is the lane that we are in. Here is something I need you board or you executive management to make a decision on to make sure that we stay within a risk appetite that we will be talking about*. That communication is absolutely critical, someone who is analytical and able to look across a wide swath of different types of risks and help to make decisions, it is a really a key attribute for a chief risk officer.

Will: So being able to get their arms around the diversity that exists in product lines, and business lines in the business, but also being able to communicate bi-directionally, helping leadership be more effective at communicating to support, helping the people who are doing technical work be effective in communicating the leadership.

Ari: I would also say normalizing across the industry. Once you decide on what those variables are that you are looking to measure. Different departments measure differently. If you are looking at a marketing function, or looking at reputational risks, it’s a different scoring mechanism than if it might be a cybersecurity risk, those sorts of things.

Will: You have a program at the Heinz College that helps people who play this role learn about these things. Could you talk a bit about that program, its inception, and the great things you are doing there?

Ari: Sure. Happy to do that. We have been looking at executive education for a long time at the Heinz College. We see it as a bridge between some of the things that we are doing in our graduate programs, some of the things that we are doing in our capstone programs, where we work with different organizations. We have been doing it since 2002. One of the first programs that we created was for IT executives, IT professionals, those folks on the path the becoming CIOs, as the part of the Clinger-Cohen Competency Act, which came out in ’96, that ushered in a variety of different types of exec ed programs for IT professionals and different aspects of the government.

When we started the program, we were one of seven schools that issued it out. It was successful from the get go, which was great, but then expanded over time to reach different types of circles. From the branch and the agencies, it went off to the contractors and the consultants who work with the federal government. Now we are seeing folks from a global audience come in from a variety of different types of companies, both for-profit and non-for-profit, as well as the government sector. We really refined the type of education that we provided.

What we saw, which was really interesting, was there was specialized needs though. You can’t just lump everything in the IT sector. Some things shake out of that. One of the things that shake out of that, was information security. They needed a specialized program, with different types of skills, different curriculum, and a different methodology associated with teaching. That’s when we approached our friends at the SEI and developed the CISO Executive Education Program. That has been going on for about five years. It has been a successful model, not just in terms of excellence around cybersecurity education for managers, professionals leading into the CISO role, but also collaboration across CMU.

We incredibly value our partnership that we have with the SEI. It has brought in this really interesting compliment of skillsets. Deep, deep knowledge in cybersecurity as well as policy and data analytics together, makes for a very powerful combination. We have running the program for five years, happy to say that we are sold-out for the next foreseeable future, every time a breach comes in we get a good 10-15 applicants. That has been wonderful. Out of that about a year and a half ago, the idea for a chief risk officer [program] came into being, and I am going to let Summer take it from there.

Summer: Yes, so some of the hallmarks of Carnegie Mellon University are looking at interdisciplinary activities, really looking at having a lot of rigor, and being forward leading. As the role of the chief risk officer has emerged in industry and in the government, Carnegie Mellon really took a step back and said, *What can we do to help fill the gap for formal education in this space*?

There is really not a lot out there to help people who are making a transition into this executive role, a C-suite level role. Carnegie Mellon said, *Let’s help fill that gap and get these people ready for this world*. If you look across the curriculum, it is exactly part of those hallmarks of being interdisciplinary. Chief risk is looking at those types of risks that Ari and I discussed.

We are not just talking about IT or finance or reputation, we are talking about all of them. We work across all of the schools here at Carnegie-Mellon and with our colleagues in industry to pull in really top-notch instructors, either practitioners who are very deep in their space, or academics who've done a lot of research. We make this a very practical program.

It is about six months long. It is a combination of being in person here on campus in Pittsburgh, Pennsylvania, and distance, but it is synchronous distance. So, you are on Tuesday nights. Your instructors are on a Webex, or an Adobe Connect session, and you are learning via that realm. You are also put into a cohort. If you are a student in the CRO program, we cap it at no more than 24 students. It is very intimate. You get to know people very well. You are put into a group of four, with three other students, and that's your team. You are given an industry or a sector and told to help build a risk program for that sector. That is our practicum project. All the things that we teach, we also do not want them to just be some sort of academic setting. It's very, very applied.

Will: The students are, for the most part, people who work in positions of this type? Or are aspiring?

Summer: Current or aspiring CROs. That is exactly what we are looking for.

Will: They have a very strong industry flavor to the contributions they make. I imagine being in one of these cohorts, one of the benefits is what you learn from the other three as much as you learn from the people you are bringing in.

Summer: Yes, it's a pretty prescriptive way that we look at how we put the teams together. We don't want to have four people from government together. As the team come in, as all of the group of students come in, we look across their backgrounds. We see their interests. We look at the sectors. We, on purpose, mix them up, so that they do have an opportunity to learn from each other.

Will: So you push outside their comfort zone. Get them outside the box.

Ari: That is the name of the game.

Will: This topic of the risk appetite assessment seems to apply here. If—let's pretend the three of us are a cohort, and we come from different perspectives—the way you would assess the appetite for risk in your organization and the outcome you'd find might be quite different from what I'd find. Could you talk a bit about this notion of risk appetite assessment?

Ari: Sure. It is an interesting concept to put something out there that everybody can agree on, what are those expectations associated with the amount of risk we are willing to adopt to achieve a strategic objective. That is where the CROs will come in, really adhering to this appetite statement, but also understanding that this is not something that's set-in-stone. This is something that could change on a regular basis. So, it has to be fluid and dynamic based on external events that occur. If the market shifts and change, their risk appetite needs to shift and change accordingly.

Summer: Yes, so this risk appetite statement is something that a chief risk officer would be responsible for developing and having the board approve that risk appetite statement. It's really something like the guardrails for the organization. As you are going down the road you want to stay within those guardrails so that you're not falling off a cliff or hitting something on the other side. As Ari said, that changes over time. Markets change, events occur, people leave, there are things outside of your power, political decisions are made and that can often require a change in either risk appetite or where your tolerance ranges are. But it really does give the entire organization a direction to head towards and to know when adjustments need to be made. So, it is setting a baseline for risk comfort for the organization.

Will: OK, pretty neat. Are there kind of cornerstone concepts similar to that that people would be looking for your program to help them learn more about?

Ari: That is a good question. What we saw, once again we have had our first inaugural cohort, and all teams did phenomenally well. Every time we go through a cohort we learn something, and we add things to the mix. *What does a risk officer need to know associated with budgeting for a full enterprise-wide-risk program?* We are adding elements to the mix.

As Summer mentioned before, this idea of social engineering is very interesting because it helps change your comfort zone, change your viewpoint associated with how you should assess these things. We are looking at including much more in-depth case studies around different companies that are involved in specific global operations. Especially if you are operating in the EU [European Union]. You cannot look at the operation in EU without understanding GDPR, General Data Protection Regulations, and what does that mean associated with changing your risk tolerance associated with operating within that region.

Summer: The two things about the program that I would say really stand out one is the practicum project that I discussed where you're put into a team of four people. At the end of the program, each team has to present to a board of directors.

This is not just a matter of, *I'm listening to the lectures and I'm putting something down in a paper*. It's a very real process that they go through in putting together this program that has to be presented to a board. There is a lot of discussion. We really try to give them a feel for what it will be like in their jobs. Maybe they have experienced it, and this is something new from a different sector. Or maybe I am aspiring to be a CRO, and I am practicing. It's a nice environment where they can get some really practical experience.

Will: So they can have a coach pushing them beyond what might have been where they would be afraid to go in the past, but they are in a safe environment where their career won't be affected by saying the wrong thing. They can really try it.

Summer: The coach is something important to note—and I'll get back to my second thing—each team does receive a coach. In addition to the world-class instruction that you get from the teachers who are teaching each of the classes, each team has a coach specific to that team to help them through the process of building the program and building their presentation. That's great.

The other thing that's really important about the program is it is forward looking. It is not just looking at what the CRO of today needs, but it's also addressing what does the CRO of tomorrow look like. Helping someone who's in the role currently, or someone who's aspiring to be there, *How do I setup things like cost saving targets?* The CRO right now, traditionally, is focused on risk and can be looked at as an expense. What we want them to be is a value-add to the company. How do they convey that to the organization? We are really helping students who are in these roles figure out, *what am I going to be in five years*? *What does this role look like in five years for my company*?

Will: Being at Carnegie Mellon is a pretty nice thing for that because there are lots of things that come to us because of the nature of the institution we are. People from around the world who are changing the world are here. You are able to fold them into the experience the students have in your programs.

Ari: Some of the stuff that we can take advantage of, because we are at Carnegie Mellon, is everything from looking at visualizing complexity to understanding behavioral organization to looking at some of the latest technologies in terms of how that might impact the risk role within an organization, especially when we look at cognitive computing, business automation, a variety of other things. We are looking at displacement. We are looking at automation of the workforce. That is a really interesting consideration when you try to understand the value at risk across the enterprise.

Will: It can go right into the insider threat and insight we have here and the effect of machine learning and other advances in how we process and learn from data. There is an evolution partly because of what you're doing, an evolution in the kind of roles and the kind of focus we have in the C-suite, and the chief risk officer is an illustration of that. You alluded to, this is a position that is facing change and has to keep up with it. What do you see as the near term, mid-term, kind of changes that chief risk officer is going face?

Summer: I can see that establishing productivity metrics for the organization will be something that a CRO really needs to be able to establish and communicate. I can also see then the translation of how do I communicate all of these diverse sets of risks in a way that makes sense to a board? The communication element, it really does often come back to that communication element, when we talk about the evolution.

Ari: Within the program we're trying to elevate the role of the CRO and get people to understand, as Summer mentioned, the business value. Change the dialog from mitigating downside risk to what is the business value associated with the program. How does it create more alignment, strategy, effectiveness, agile nature, associated with the enterprise going forward?

We tend to take a look at, *What are the industry benchmarks? Who does a CRO report into? Where do they get their budget from? How does a budget get assessed?* Those sorts of things, because, as we are seeing multi-complex organizations, there's a CRO but there's also a bunch of C blank, blank O's as well that are competing for a variety of different types of budgets, resources, and consideration from the board. We are trying to understand all that and trying to figure out how to elevate that role.

Will: Is it safe to say that the opposite side of risk is not status quo but really opportunity? That is the payoff that we want to be able to demonstrate. It's not just eliminating the negative, but finding a leverage for the positive, right? I sound like a slogan.

Summer: Absolutely. Looking at opportunity as the opposite of risk, how do I then leverage what I know so that I am achieving a value-add by capitalizing on those opportunities?

Ari: It is also, I think, opportunistic if you look at today's business environment and all the disruptions that are occurring on a constant basis. Before we might have seen black swan events happen rarely, now we're seeing them happen frequently. Consequently, it just proves that the role of the risk officer is becoming more and more necessary in terms of enterprise strategic planning and understanding how to quickly create resiliency and adaption, which is critical for any industry operating today.

Will: What do you see coming in the future in terms of the evolution of your program for the cohorts that will come in once you have graduated a few more and space is available to sign up?

Summer: As Ari noted, every time we run a cohort we go through an update of the curriculum and say, *All right, were there hits? Did we miss anything? Were there big hits? What are some things that we need to add?* We are going through that now. We are looking at some of the future of a CRO and pulling in some information and guest speakers that will really hit on things towards the value-add.

The list of professors that we have is phenomenal. We have from some of the biggest financial institutions, acting CROs, people who are in the CRO role right now. We have an astronaut from campus who teaches. Who knows more about risk than an astronaut? We have a wide swath of really neat experts.

What is really key about the program, though, is the cohort model and the fact that you get to know 23 other people who have common interests. The students really learn to lean on each other. They are building a network. Then you become a part of the CMU community. Now they do not just have the other 23 in class, but they have all the cohorts that graduated before them, the cohorts that are in other programs. What we have seen is this fantastic network that has grown of professionals in the C-suite. They have helped each other get jobs. They have celebrated each other's successes. They've written articles about each other in the paper. In fact, this program was written up not long ago in the *Wall Street Journal Pro*. In the cybersecurity area. One of our graduates Rob Sloan, wrote an article and interviewed several of us about that. There is a lot of opportunity for exposure and networking and learning from your peers.

Ari: I'd like to see the same progression we have seen in some of our other exec ed programs. There is a lot of value in risk folks getting together from different organizations, but there is even more value when you bring in folks from the legal side, from the operations, from the tactical side, to get them to understand the risk function within an enterprise. That adds to the social engineering around and the complementary skill sets associated with bringing them in to really create more of a holistic understanding what does risk mean across an organization.

Summer and I also love doing critical thinking, critical reasoning exercises. I think that's great because to really understand the climate, the business operation climate that you are dealing with as well as the inside enterprise climate that you are dealing with, you have to ask a variety of questions. You need to draw that out through this role-playing exercise where you are doing critical thinking, critical reasoning, design thinking, parallel thinking, and those sorts of things. I think there are opportunities to roll that into the program so that we can get them really asking these questions around ethicality, around society, and what is the benefit associated with the societal or the organizational impact around some of these programs.

Third, I think there is always an opportunity to do interesting analytics. Maybe it is part of where I'm from, but I think communicating complex risk matter is really difficult. If you can do that intuitively through digital storytelling around data and allow people to engage with the elements. So if they move something from one area to another area, *If I take this pot of money from this risk program to this risk program, what happens to overall risk?* Well, now I intuitively know what is happening because I'm actually moving these elements around and integrating. So I am cognitively processing what would happen. I think that is a wonderful and interesting area to explore in the future.

Will: That would seem to focus on making things more concrete, more tangible, more accessible, while, at the same time, your previous point was to bring a greater diversity of perspectives to help people understand from more than one view the phenomenon we are trying to manage here.

Ari: If you are on a board or you are a CEO and you have a chief risk officer or you are looking to get a chief risk officer, it is the kind of program that you really want to send your people to because we are teaching them the critical thinking and the deep skills. But we are also constantly reminding them, *You are doing this for the goals of the business*. We are helping them keep their eye on the ball or, *There are business objectives that we are trying to achieve*. It is not that you are doing this in a vacuum. So it is all of these skills pulled together to achieve the end game.

Summer: So, it is not something you learn by rote and then repeat, rinse and repeat over and over again. It's something you really need to understand where you are, what the context is and apply it as appropriate.

Will: If you are a CRO of one company and you move to another company, it is going to be different in how the execution occurs. We're teaching the fundamentals that can translate to any of those platforms.

Will: Ok, great. I would like to thank you both for coming in. It has been very interesting today.

Ari: Thanks, Will.

Summer: Thank you.

Will: If you'd like to learn more about the program we've been discussing, you can look for information on the Chief Risk Officer Certificate Program on the Heinz College website at www.heinz.cmu.edu/programs. Also, an Internet search for chief risk officer will likely turn up that program as well. I am told it is often the first result when you do a search.

Please know also, that we will provide links and references for information we have discussed here today. The transcript of this podcast is available for download on our website. As always, you can go to sei.cmu.edu/podcasts for a full listing of this and other podcasts available as well as on Carnegie Mellon University's iTunes U site and finally on SEI's YouTube Channel. As always, if you have questions, please don't hesitate us an email at info@sei.cmu.edu.