Structuring the Chief Information Security Officer Organization
Transcript

Part 1: Four Key Functions

Lisa Young: Welcome to CERTs 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.

My name is Lisa Young. I'm a member of CERT's Cyber Risk Management team. I'm pleased to welcome back my colleagues Julia Allen and Nader Mehravari, also members of CERT's Cyber Risk Management team.

Today, we'll be discussing a recent report they have authored, along with several others, titled *Structuring the Chief Information Security Officer Organization*.

Welcome back to the podcast series, Julia.

Julia Allen: Hi Lisa, it's good to be here. And it's nice to have you as the moderator instead of me.

Lisa Young: I know, and thank you so much. And Nader, glad to have you with us today.

Nader Mehravari: Always good to be here and thanks for having Julia and I here for this conversation.

Lisa Young: Well we're very happy that you could be with us today. And so, this technical report that I've read, it seems that there's a very wide range of things that Chief Information Security Officers (CISOs) have under their purview and that they're responsible for. So, starting with you Nader, can you talk about how did you go about identifying the key functions that cover most of a CISO's responsibility?

Nader Mehravari: As part of our larger organization's mission, we continue to observe the environment and learn from other organization's experiences. And so, we start by observing the fact that traditional strategies and functions that are typically used by information security teams and their leaders are no longer as effective in dealing with the risk environment that we all operate in. So, based on those observations, we have characterized or defined four key functions that any modern information security team should seriously consider.

Traditionally, information security teams have been tasked to protect the organization's information assets by trying to prevent cyber incidents from taking place. Over the past several years, the community has clearly learned that regardless of how much investment is put in place to protect themselves, cyber-attacks do take place.

Lisa Young: Right.

Nader Mehravari: They negatively affect the organization's mission. Now, don't get me wrong. That function needs to continue, and it's critically important for organizations to put in place a very comprehensive set of mechanisms to protect and shield themselves from cyber threats. That is the first function.

Lisa Young: Okay. Protect and shield.

Nader Mehravari: Right. But we know these functions often are not as successful, and they often fail. And given the nature of this foundational function that we've been looking at, we have identified two other functions. In real life experiences from industry and by some analysis, and by research, it's very clear to us and others that it often takes a long time for organizations to detect that there has been an intrusion, or that there has been a cyber-attack. In fact sometimes it takes weeks or months for them to be identified. And therefore, organizations have to become better and more focused in monitoring and detecting these incidents. They have to become hunters. Hunt for the adversaries. So, that's the second function that we have identified.

Lisa Young: All right. So, monitor, hunt, and detect, as second function.

Nader Mehravari: Right.

Lisa Young: That sounds great. All right, what's next?

Nader Mehravari: And then, clearly today's cyber adversaries are becoming more interested in things other than just stealing data or exposing sensitive information. Unfortunately, they're becoming interested in disrupting organization's day-to-day business function. They've become interested in making operational havoc, including making physical damage. And therefore, information security teams must be prepared to respond to disruptions of business operations. They have to incorporate their activities with other contingency planning that's done in the organization. And this is the third function.

Lisa Young: Okay. So, that respond, recover, sustain function, that's a really important key function. And what's next then?

Nader Mehravari: And finally, the fourth function, the community has learned that tools and technologies, although necessary, are not sufficient. We can throw all the tools and technology we want at the problem. Organizations will not be fully successful in their information security mission. And therefore, they must ensure that there is an integrated set of policies, oversight functions, process improvement, risk management practices, and measurements are in place to support the other three functions. This serves to put it all together into four key functions that we've identified as a modern information security team to consider.

Lisa Young: Okay. So, protect, monitor, respond, and govern, that's really great. Julia, do you have anything to add?

Julia Allen: No, Lisa, but I'm ready to put the meat on the bones.

Part 2: Departments, Functions, Sub-functions, and Activities

Lisa Young: All right. So then Julia, can you tell us about the sources that you used to fully describe the scope of each of these functions?

Julia Allen: Sure, Lisa. So, you have four functions and that's all fine and well. But the devil is always in the details, right? So, what does it mean to operationally and prescriptively enact each of the four functions that Nader described?

So, the way that we tackled this is we considered credible, reputable, reliable sources of information security practice. And I'll just briefly touch on these. They're discussed in more detail in our report. So, a typical large diverse organization's information security policy, what topics are generally in that policy? We certainly looked to NIST, the U.S. National Institute of Standards and Technology, has a wealth of information, particularly their special publication 800-53 on security and privacy controls and the Cyber Security Framework that's getting a fair amount of traction in the U.S.

For workforce development, because it always comes down to people, we looked at the National Initiative for Cyber Security Education, the NICE workforce and framework. A real popular set of security controls is what is typically called the SANS top 20, the SANS critical security controls. We mapped to that. And then we would be remiss if we didn't take some of our favorites. So, our own CERT Resilience Management Model (CERT-RMM) serves as a foundational document for fleshing out each of these functions.

And over the years, the Department of Energy has embraced that construct and developed a series of models including the Cyber Security Capability Maturity Model (C2M2). So, we map to that as well. I'd be remiss if I didn't mention that we did not specifically map to the ISO 27001 and -2 series because we felt that all the other sources covered the kinds of practices and processes that are recommended in the ISO series. But those are the sources we used to really flesh out, Lisa, what each of these functions entailed.

Lisa Young: Okay, well that's quite a bit of research there, and very many good sources. So, thank you for that Julia. So, then back to Nader. So, Nader let's talk about -- would you briefly describe the process the team went through to develop a CISO organizational structure?

Nader Mehravari: So, we started our conversation by describing those four key functions. And Julia just mentioned some of the input that we are using through the process. So, if you look at the overall process, it was actually a relatively structured approach that our team took. We started the process by considering input and observations from the information security community. Clearly, what CISOs and security professionals experience on a day-to-day basis is important. And therefore, with our work with other organizations, we have some observation and information from practitioners in the field.

Our team from time to time looks at certain major cyber incidents and does a little bit more analysis and research into details of them, plausible causes, what worked, what didn't work. So, we have that information.

Lisa Young: So, there's no shortage of -- sorry to interrupt. There's certainly no shortage of recent cyber incidents for sure.

Nader Mehravari: Right. In fact, we could spend all of our time doing that.

Lisa Young: All right, and then what else did the team do?

Nader Mehravari: And then as teams that we pay a lot of attention to, risk and risk management, and the risk environment, we continuously learn not only from information security professionals, but other operational risk management activities, what's happening to the risk environment. So, we considered that.

So, those were high level inputs to the process. Those high level inputs helped us to define those four functions that I described earlier. And then it was time to take a couple layers of

onion off. The first layer of onion we took off we considered those inputs that Julia described. And we tried to map these existing codes of practice, or standards, or framework, whatever you call them, we map their specific topics to one or more of those four functions.

Lisa Young: Okay.

Nader Mehravari: Once we started doing that, we realized we are developing a very large matrix or spreadsheet of high level things, then four key functions. Then as we took additional layers of onion off, we noticed things that can be organized into a "department," or things that can be organized into "functions", "sub functions." And then that's how we continued the process. So, start at the high level input, define the four functions, and then using the existing codes of practice to develop detailed information.

Lisa Young: And refine that then into different buckets. Okay, well great. Thank you for that. So, then Julia, back to you. Thinking about all we've gotten to so far, can you say what is the result or the recommended structure for a CISO organization that resulted from the process that you all have described?

Julia Allen: Sure, Lisa. But if I may just let me add one more thing to what Nader was talking about. When we were doing this kind of large mapping, affinity grouping, creating all these buckets of activity, we also did, I think, one interesting thing where we also suggest activities or sub functions that could be outsourced, that could be done by another part of the organization. Or maybe it's specifically done by IT. Or maybe it could be done by a managed security service provider. But the important thing to note there is that the CISO still retains oversight responsibility even if something is being done by a third party inside or outside of the organization. So, I did want to mention that.

Lisa Young: Well, I'm glad you brought that up. Can we stay there just for a moment and talk about that? Because more and more organizations now are starting to see that certain services, whether they're provided by IT or an external provider, can be outsourced. And so, I think that it's important to make that distinction whether they're done inside the organization or outside, that that governance and oversight and leadership should still be provided by the CISO organization.

Julia Allen: Right, and one of the critical things that Nader talked about when he was describing that fourth function is the whole idea of measurement. And the idea is that if a CISO retains and is responsible for this oversight responsibility, one of the ways to enact that is to ensure there's a consistent set of metrics that they use within the organization, but also with their vendors and suppliers and contractors.

Part 3: Candidate Organizational Structure

Lisa Young: Oh, that's a great point. So, thank you for bringing that back up because that -- everyone's always asking for security metrics. So, this can give them some idea of how that might be structured and how to maintain that. Well, then so talk about what is the recommended organizational structure that resulted from the process you described.

Julia Allen: Sure, I'll touch on this briefly. And there's a lot more details in the report about what each block in the org chart typifies. But clearly, you start out with the CISO and perhaps that's indication of where that role reports into. There are all kinds of debates about the right place for where the CISO is supposed to report. But we really go from the CISO down, allow for them to

have a deputy and perhaps an information security executive council as an advisory board that Nader will talk about in a moment.

And then we have basically four blocks or four next level reports to the CISO, program management, the security operations center, the emergency ops and incident management group, and what we call security engineering and asset security. So, let me just give you a quick one or two lines one each of those. So, program management has just overall management responsibility, governance, risk and compliance. We put workforce and supplier management there. And the interface with the rest of the business.

The security ops center is pretty familiar to most folks. It works very closely with IT and is sometimes partially performed by IT where it does situational awareness, ongoing monitoring the security helpdesk, which might be the first line of defense for the computer incident response team.

The reason we wanted to really have a separate emergency ops and incident management center is it works closely, obviously, with the security ops center. But it mobilizes the organization for high impact incidents. And when that's not happening, it's doing conscientious planning for incident response, business continuity, disaster recovery, running tests and exercises and drills, and also will do the post mortem on big incidents and investigations.

And last but not least, security engineering and asset security, that covers whole lifecycle of an asset, so from birth to death, from development and acquisition all the way through operations. It's a big function. We put it together for a reason which I'll talk about a little bit more later. But it has everything focused on making sure an asset, information, technology, applications, networks, facilities are secure for their entire lifecycle, their entire period of operation. So, that's a brief description of the recommended structure that we've developed.

Lisa Young: Okay well, great. Thank you so much for that. So, then Nader, Julia mentioned the CISO and perhaps the deputy CISO possibly being assisted or enhanced by an information security executive council. Can you say something about what's the role of that council and how they might assist in this process?

Nader Mehravari: Yes, we think that's actually a very important consideration for information security organizations. We have labeled in our report an executive council. Other entities may give it a different name. They may call it an advisory council. Some organizations have an internal version and an external version. They may refer to the external version as maybe the industry advisory council.

Regardless of what it ends up to be labeled, it becomes responsible for advising the chief information security officer, helping he or she to ensure a few things, ensuring, for example, that the information security principles and practices and activities are aligned with the larger organization's business objectives, ensuring that the information security objectives that have been set are being met, ensuring, for example, externally or internally imposed policy and compliance obligations are considered and met.

So, it provides lots of advising, things that maybe CISO, although pays attention on a day to day basis, it would be good for a second pair of eyes and guidance to be provided from time to time from those who may have other types of responsibilities and visibility in the enterprise.

Lisa Young: Sure. So, that takes us back to that notion of governance. I mean this is very key to making sure that the CISO has some support for governance.

Nader Mehravari: Right, in fact, we mentioned one of the four key functions in a modern CISO organization is that governance function. And we think having an executive council is a good aspect of that governance and oversight responsibility. And we often get a question asked who should be on these type of executive advisory councils. Clearly, you want individuals who have visibility into other parts of the organization or have visibility into things that are very much related to information security. So, clearly, chief information officer, or chief privacy officer or the position who is responsible of physical security are good candidates for membership on this executive council.

And then from a business perspective, you clearly want to consider chief operating officer who worries about day to day business operations. From legal perspective, having the general counsel to be a member is a really good idea. From a perspective of support structure, human resource executive, or communication department, those are all good examples of type of individuals or positions who would serve on the executive council.

Part 4: Security Engineering and Ops; Next Steps

Lisa Young: Thank you for that. That's really helpful. So, thank you for laying that out, the role and the candidate positions for that.

So, then Julia, back to you, you mentioned a few minutes ago about the security engineering and asset security and this lifecycle approach to that. Can you talk more about why did you recommend that security engineering and asset security be combined, and what that might look like or why that's important?

Julia Allen: Sure, Lisa. And this is probably one of the areas that may not be traditionally implemented in most organizations. Typically, you have the folks responsible for development and maybe even acquisition very separate and distinct from your operational or IT shop. And so, in this particular part of our structure, we've put those together. And the reason that we've put them together is because what has been happening with movements like the DevOps movement where you don't have the folks developing and acquiring software, throwing it over the wall to IT saying, "Good luck, Godspeed, and whatever happens, it's over to you."

I think the community is finding with how fast these systems are occurring, with mashups, with Agile, with all the different approaches where you are getting, in some instances in high performing organizations, multiple releases of new features and new capability every day, your development and acquisition side of the house really needs to be very tightly integrated with your IT ops.

And so, we've put the asset centric functions of security engineering, how you develop security through requirements architecture, design, and release phases, together with identity and access management, application security, host and network security, information asset security, and at least the access control aspect of physical-- accessing physical facilities. And we are encouraging those considering this approach to at least take a look at putting those functions more tightly coupled organizationally.

That said, many CISOs have different skill sets, have different leadership structures. And they may not be able to do that. But they should really take a look at a much tighter coupling even if they're in several different parts of the organization, look at a much tighter coupling of those functions and capabilities.

Lisa Young: Well, thank you. And if you have anything to elaborate on from a security engineering -- I like the title, security engineering. To me it means that you're going to engineer thoughtful security into this. Is there anything else you want to say? I know that's something we've talked about over the years in our development, about actually having an engineering process related to security in totality.

Julia Allen: We have a whole body of work within CERT and certainly other places in the communities that are tackling that part of the lifecycle and, as you said, thinking about security from the very beginning all the way through to operational deployment. Sometimes we'll refer to that as software assurance. So, for folks who are interested, there's a very rich body of knowledge both at CERT and in the community about how do that capably. And we highly recommend putting those together.

In the CERT Resilience Management Model, we actually have a process area called Resilient Technical Solution Engineering (RTSE) that addresses early lifecycle to try and build that bridge between early lifecycle phases and operations.

Lisa Young: Okay, great. Thank you for that. Thank you for the elaboration. Okay, then Nader, thinking about all the things we've discussed today, for a CISO who wants to use this approach, or at least get -- what are some recommended next steps that they might take?

Nader Mehravari: Like many other things in risk management, information security, and so on, the exact manner by which some of these recommendations or approaches should be put into practice are dependent on the nature of the organization. But here's one typical set of steps that can be considered to put some of these ideas into practice.

Maybe the first step would be that the information security organization or the Chief Information Security Officer would try to map how their current structure is to these four functions that we have defined and the departments and sub functions and activities that we have described. That could be the first step, how do these recommended structures map to their current structure.

Lisa Young: So, that could also maybe provide -- just doing that one step might also provide the CISO a comprehensive way of looking at their own programs to make sure there's no gaps.

Nader Mehravari: Exactly. In fact, that could also be considered one of the first steps in an overall process improvement in a sense of identifying where you are and how you compare to other things.

Lisa Young: Okay.

Nader Mehravari: So, a typical second step could be that the organization determines what units should continue as they are, what units need to be changed. And the change could be making it bigger, making them smaller. And then what functions are missing? So, do that analysis as a second step. This second step usually results in ideas about what to do and what steps need to be taken.

And that leads itself to a third step of developing an implementation roadmap. Usually, you're going to come up with a long list of things that should be done, analyzing them, and put them in order, which ones are important, which ones can done now, which ones should be done next year, and develop a roadmap.

In developing a roadmap, there are existing codes of practice and guidance that can be used to help organizations to do that. Julia referred to some of these sources. The CERT Resilience Management Model is one place that organizations can go to learn about how to implement some of these ideas. Or they can go to the Department of Energy's work under Cybersecurity Capability Maturity Model, or the Department of Homeland Security's Cyber Resilience Review program. These are all sources that could assist the CISOs to implement the roadmap that they come up with.

Lisa Young: Okay, that's great. Thank you so much for that. Julia, anything to add?

Julia Allen: No, Lisa, other than as we come to our close just really we would love to hear from anyone who's tried to take this for a test run and has additional steps or activities that they did that they might find useful that we could use to augment this body of work.

Lisa Young: Okay, thank you. So, then I'll ask each of you separately, but can you tell us, Nader, starting with you, where can our listeners learn more?

Nader Mehravari: So, as both you and Julia had mentioned, we have a recently published technical report that's available for folks to take a look at. We have developed a set of presentation slides that we can make available to interested parties. And Julia and I recently delivered a webinar that has been recorded. And it's available for replay.

And before I forget, I mentioned at the very beginning of our conversation that we had benefited by having discussions and observations from other organizations. And one of those organizations who contributed a lot to our understanding of the issue and the subject is U.S. Postal Service. We have been fortunate to collaborate with them for a long time on different operational resilience and risk management issues including cybersecurity, and in particular contributions of the sponsor of those activities, Greg Crabb, should be mentioned.

Lisa Young: All right, thank you for that. And Julia, anything to add about where our listeners can learn more?

Julia Allen: The only other thing I wanted to mention, Lisa, is I heard from some of our SEI folks who helped get the word out on our body of work that when they put the Twitter feed up on this particular topic and report, there was a lot of interest. And as a result of that, we'll also be doing an SEI blog at some point in the future that also describes this body of work. So there'll be a lot of resources out there for people to take advantage of.

Lisa Young: Okay, great. All right, thank you both so much for that. All right, well I think that brings us to the end of our recording today.

Thank you so much both for being here. We really appreciate your time and energy on this.

Julia Allen: You're welcome, Lisa. Great to be with you.

Nader Mehravari: Thank you.