How the University of Pittsburgh Is Using the NIST Cybersecurity Framework Transcript

Part 1: Applicability of the NIST CSF

Lisa Young: Welcome to the CERT 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 the CERT Cyber Risk Management Team. I'm pleased to welcome Sean Sweeney. Sean is the Information Security Officer (CISO) for the University of Pittsburgh. Today we will be discussing Sean's use of the NIST, National Institute of Standards and Technology, Cybersecurity Framework (CSF) for helping manage his organization's cybersecurity risk.

Welcome to the podcast series, Sean.

Sean Sweeney: Thanks, Lisa, and I'm glad to be here and I'm really looking forward to the opportunity to speak to you and eventually the audience about what we were doing with the NIST CSF here at Pitt.

Lisa Young: Thank you. So on that note, would you give us a brief overview of the risk environment at the University of Pittsburgh?

Sean Sweeney: Sure, sure. Higher Ed, especially a research institution of our size, is a different beast than I think most consider and it does present some challenges when it comes to securing an environment like this.

The university itself, just to set the stage, we have approximately35,000 students and another 13,000 faculty and staff. They're spread across five campuses, but most of them are here in our Pittsburgh campus in Oakland. Universities, by their very nature, are largely decentralized beasts. I often say I'm not the CISO of a corporation, I'm the CISO of a city-state. Because we really are -- it's up to sixty different organizations under the same umbrella and we have facilities, we have the business units, we have the academic units, those that are doing research, so on and so forth.

Some of the things that make that challenging beyond what I just said, would be Higher Ed -- we really are -- we're a target rich environment. First and foremost, since we're a research institution the size and speed of our network is just amazing. And, honestly, it's one of the first things that struck me when I first came here almost three years ago. So we're built for large data transfers, lots of nodes on the network -- I have 300,000 end points on my network at any given time.

Lisa Young: Yeah, that's a lot.

Sean Sweeney: Yeah! It's a lot to keep track of. It certainly is. And then you throw on top of that just the whole collaborative nature of research and academia, in general. The whole idea of academic freedom runs completely contrary to the black and white security.

Lisa Young: Well, I was just gonna say, that's a lot of diversity, a lot of different kinds of things you have to deal with. So that city- state is appropriate moniker.

Sean Sweeney: And that's absolutely true and then the other thing, and you just hit on it right there, is the diversity, not just in the different groups here, but what comes out of that is the diversity in the information that they're working with, right? I used to often joke with some friends here in town that were in security at a local financial institution, that their job was a lot easier than mine, because their network was built to do one thing and that's facilitate financial transactions. Mine is built to do 200 different things.

We've got some very traditional business units that you would find in the corporate arena. We've got the CFO's office that does all the accounting and the general ledger, all that type of stuff. You have admissions and financial aid, you have the registrar's office, you have student financials -- very academic-specific, but still business functions. But then you throw in, we've got health sciences, we've got engineering, we've got social science research going on, all of which may have their own intricacies, their own different definitions of what is sensitive. And then throw on top of that most of that work's being done under grants or contracts, which may or may not come with their own security language.

Lisa Young: Right, well, that's definitely a target-rich environment. So then how did you first become aware of the NIST Cybers800-03ecurity Framework, and what made you think it would address the diversity of your risk management and cybersecurity needs?

Sean Sweeney: Sure, so, we have been -- I have been familiar with the various publications from NIST when I first got here, because one of the first things we had to do is because we receive a lot of contracts from federal agencies like NIH (National Institutes of Health), we're seeing some flow-down language, specific to FISMA (Federal Information Security Management Act). So we had got involved with the -800*8+series document from NIST.

And then our chancellor retired and they had selected the new chancellor who happened to be the former director of NIST, which obviously got my attention. And then we saw the publication come out. I believe it was February 2014. Prior to that, the president had issued an executive order and policy directive setting the stage for the critical infrastructure and setting the stage for NIST to create this document. So when it came out -- quite frankly we were very interested in -- even if just from an academic point of view seeing what it was. And then when we dug into it, obviously, it seemed like it would fit the environment being that we're so diverse here, trying to shoehorn frameworks here in the past had always been something that was difficult and the framework seemed to offer us the flexibility to do so.

Lisa Young: Right. That's a great thing. So then talking about that framework, can you say how did you get started on using the framework?

Sean Sweeney: Sure. Well, so the first thing is the framework itself -- I should take a step back and talk about the framework, how it's designed, because that flows into how we used it.

Lisa Young: Sure.

Sean Sweeney: So the framework consists of five core functions and they're Identify, Protect, Detect, Respond and Recover, right? So those five functions are broken down into categories and then subcategories. An example of a category would be asset management. An example of the first asset management subcategory, I believe, off the top of my head it says, "Hardware

and systems will be inventoried," right? So it's like a control, but it's not prescriptive as much as it is descriptive.

So you've got that core, and then there's also this concept of these implementation tiers and they'll actually come into play when I talk a little bit later about how we use this at the university, but those are risk tiers and they're -- because the whole point of the framework is to measure your program and also inform risk. But the real meat of the work that happens with the framework is taking those core functions, categories, and subcategories, and then creating what's called a current profile...

Lisa Young: Yes, please, tell us about the profile and how that applied to your environment.

Sean Sweeney: Okay, so when you work with these -- we'll call them subcategories -- you take all those and you compare them to your environment. You basically go through and take these descriptive -- I'll call them "controls" for a lack of a better term, but they're really not control objectives, but you take these…

Lisa Young: More like practices, right?

Sean Sweeney: Yeah, exactly. Exactly.

Lisa Young: So I would say they are more like practices you would want to do in a framework that would set the stage for controls as well as other activities, right?

Sean Sweeney: Exactly, exactly. And, in fact, the subcategories actually do map to specific controls from various standards, like COBIT, ISO, 800-53, so on and so forth. So you go through this current profile exercise and it's -- you write down how you're doing, how you're meeting all of these descriptive practices. And I had to work with not just my security team, because we were doing it from -- we're central IT here at the university -- so we were doing it from an enterprise level, although that's kind of misleading because universities are so decentralized.

We are in charge of the enterprise applications and the network, which is an enterprise service. But we don't control all of the end points. So we were just doing it, Phase 1, from our point of view -- those things that we did control. So I worked with other directors in our IT group and then filled out this current profile.

Then what you do is you go through that current profile and you do a risk assessment. And it's funny though, because even before you get to that risk assessment phase, as soon as you write your current profile -- like, your current answer, you immediately want to, your brain goes, "Oh, my god, I know a better way to do that," or "Oh, we should be doing this." And what that translates to is after that risk assessment, you're supposed to create a target profile, right, which is where you want to be. So it was just funny because it was really difficult to not jump to that next step before the risk assessment in the middle.

Part 2: Assessment, Current State, and Desired Target State

Lisa Young: So then would you say conducting the risk assessment -- so that gave you a sense of where you are, your current as-is state as in the document?

Sean Sweeney: Yeah. Right. That gives you your as-is and then you -- then you list out your -- and I don't want to call it a dream state, because you don't want to go pie in the sky. I told my

team if we were to take it to the next level, what would it look like for each of those subcategories?

Lisa Young: So that's a really good. So say the categories then one more time and subcategories just to -- for our listeners and for me just to catch up here. So: identify--

Sean Sweeney: Sure. So the function is identify, the category is asset management, okay? And then the first subcategory for asset management - is ID AM-1. And it's --

Lisa Young: Okay.

Sean Sweeney: -- physical devices and systems within the organization are inventoried. And so…

Lisa Young: When you looked at your current profile in that area, those practices -- that helped you identify where you were today.

Sean Sweeney: Right, right. We went through and we listed out all of the various systems and policies related to that practice here at the university and that was summarized in a narrative form with supporting documentation in our current profile.

Lisa Young: Okay, that's great. And then what happened?

Sean Sweeney: And then, based on writing that and based on a risk assessment as well as just common sense best practices, we then had to go through the target profile exercise. So taking that same subcategory as an example, so we listed all these different systems that were meeting this practice of physical devices and systems are inventoried and supporting policies. But we recognized that, through the current profile, that it was multiple systems, they weren't talking to each other, there was a lot of room for potential error, and it was supported by various groups within central ITs' standard operating procedure, not a larger policy.

Then the current profile becomes, -- we need to design a way to do this in, at least, a grouping of systems that interact with each other and are done under a single, standard operating procedure within the department governing the inventory of assets, right?

Lisa Young: So then, thinking about your target profile, what are some of the actions that you took then after you identified your as-is state, then to think about what your target profile should be?

Sean Sweeney: There's a cross-walk to other control families, other frameworks, and so some of it you could -- we did turn and look at those, look at what, for that specific example, what COBIT controls were listed? What ISO controls were listed? What did the 800 53` have to say about that? And then also just knowing our environment, knowing our risk tolerance, knowing the culture here, in terms of how we build things, how we manage things, how would we want to take that to the next level and then that became what our current profile, for that specific subcategory was and then we went all the way down the list, took our first stab at that, but then we had to go back to the stakeholders -- in this case it was other IT directors within a central IT organization -- and say, "Are we out of our minds?!"

You know what I mean? Like, "Is this something that we can accomplish under the best circumstances and the worst circumstances?" and there was some editing that went on. There was some -- security had to give a little, some of the departments had to give a little to come up

with that desired state, what that would look like. And then the important thing to remember though is that entire desired state, that whole current profile, the idea isn't that -- I mean, that's where you want to get, but obviously we talked -- there's 98 subcategories; we can't do all that Day One. So you have to really go through and do a prioritization and it is from that prioritization that we got our list of to-do's, right? And then proceeded from there.

Lisa Young: So can you say more about that prioritization process and how the discussions went with some of the other groups in your organization? Because it sounds like there's a lot of good stuff in the NIST CSF.

Sean Sweeney: The NIST CSF as it is, by itself, is purely a qualitative exercise. So it doesn't give you the ability to -- you can't put it in a heat map, or anything like that, and see where visually where you need to redress. So you have to do it -- we took it function by function and we looked at, of the gaps between our current and target profile in this function, in identify, what presents the most risk to the university -- and, I'll be honest, some of it was "What is some low hanging fruit that still provides value that's also in this list?" And then we prioritized that and we did that for each of the functions to come up with the hit list of what we were going to work on next.

Part 3: Early Successes and Lessons Learned

Lisa Young: So what were some of your early successes or results by doing that?

Sean Sweeney: Really most of it was taking existing practices and streamlining them, documenting them a little bit better. In some cases, like in the case of the asset management, making sure that we already had a system of record that was enshrined in policy as a system of record, but not -- and that wasn't being as used like it necessarily should. So going through and fixing that. Other things were expanding programs, for example, our vulnerability management programs, both at, for web applications and for hosts, taking them from an ad hoc on-demand type of thing, and turning them into a more robust, repeatable, continuous, program.

Lisa Young: I was just going to say that sounds like it could add a lot of value to your cybersecurity program across the diverse environment you have.

Sean Sweeney: Absolutely. Absolutely. And, doing it at Phase was doing it, like, this enterprise level, but I always recognized that we're just a piece of the puzzle, right? -- A big piece but still a piece of the puzzle. But I have -- even though I'm in central IT, I have responsibility for the security across the entire university.

So we have all these departmental IT groups that have work stations, in some cases, servers that are still on campus or servers that they're managing at our network operations center. And they have a lot of risk there, too. So I had to -- I knew from day one that I was going to have to come up with a way to make this CSF exercise at the enterprise level bubble down to the departmental level.

Lisa Young: Okay, great. So then thinking about all that you've told us today, what advice would you have for someone who wants to use the NIST cybersecurity framework to manage their cybersecurity risk? How can they get started and what might -- advice would you give them?

Sean Sweeney: I would, first of all, definitely encourage it. We're a big believer here of the CSF, mainly because it allows communication of cyber risk up, down and across the organization and because it is so descriptive and not prescriptive. So in terms of what to do, obviously first, you want to go to the NIST CSF website, download the framework. It's still in its first version, but also on that website -- and this is one of the cool things about the CSF is that it's evolving -- just like the current and target profile documents that we created, are a living document. We're constantly updating them, specifically every quarter; the CSF is still evolving, too. So NIST has on the CSF page, they actually have a road map so you can get an understanding of the key areas of development, alignment, and collaboration and you can have -- because of that collaboration, you can actually have a hand in that.

So just taking the CSF and reading it and figuring how you -- I mean, ideally, you would just pick up and create a target and current profile. That said, that might not be as easy for all organizations and so DHS actually has what they call their C voluntary program. It's Critical infrastructure Cyber Community voluntary program. They have an on-site and a self- guided -- what they call their Cyber Resilience Review, which is based on the (CERT) RMM (Resilience Management Model), but also maps to the NIST CSF. And so they have a lot of great resources, that, again, either on-site or self-guided that can help an organization go through this process.

And they also hold -- and I attend these -- they hold, I believe its quarterly -- calls where different groups from the critical infrastructure sectors come together and discuss -- usually there's a couple of presentations. I think the last one I saw was someone from the energy sector presenting on how they were adapting the NIST CSF to their sector and how that's going to flow down to all the individual companies that make up that sector

Lisa Young: It sounds like then the NIST Cybersecurity Framework can be used alongside other frameworks and things that you have. Were you using any other frameworks or have you since added any frameworks to your use of the NIST Cybersecurity Framework to address your diverse environment

Sean Sweeney: We weren't using -- and we had looked at other frameworks to determine how we could apply them to the university, but what we realized is as they existed by themselves we were going to have to do some extreme hybridization of those frameworks to be able to fit into all the nooks and crannies that is the University of Pittsburgh. That said, though, the CSF does lend itself for mash-ups with almost anything. And a great example of this is -- there's a regulatory group. I think it's the FFIEC (Federal Financial Institutions Examination Council) for the financial industry mashed up the Cybersecurity Framework with their existing security documentation.

And the cool thing about it was -- and you remember earlier I said I had to figure out how do I get this enterprise activity down at the department level and then really from -- when I say things like that, what I mean is "How do I do it scalably?" right? Because I only have a certain number of people in security that, and I can't send them -- abandon all their duties to go do the CSF exercise with200 different departments. What this group did is they did this mash-up and for each of those subcategories, they gave acceptable answers. And they did one through five; I'm going to do one through four. And what that allowed is turning the CSF into a quantitative exercise as opposed to just a qualitative exercise.

So that's actually what we're working on now to push down a self-service tool to the departments to use and it's just an example of the flexibility of the CSF and the fact that it's still living and breathing itself, which I honestly think is the purpose of it, right

Lisa Young: Right

Sean Sweeney: Strengthen the cybersecurity of critical infrastructure across the United States and so it's not rigid at all, so it allows people to adopt it and make it their own, but still we're all speaking the same language

Lisa Young: Sure, so that descriptive quality you described, that actually seems to me, like, it would be a really good way to talk about -- to raise the bar, so to speak -- to talk to people about all the different kinds of things they should think about when managing cybersecurity risks.

Sean Sweeney: Absolutely. Absolutely. And, like I said, it allows you to communicate with the same language up and down an organization, but also, ideally, across an organization. And for someone, like a university, where -- education isn't its own critical infrastructure sector, but we play in almost all of the other critical infrastructure sectors, right?

So it'll allow us to talk to, hopefully, the NIH with the same language. It will allow us to talk to FERC (Federal Energy Regulatory Commission) with the same -- and it doesn't even have to be a government organization. It can be any of the groups that we work with. So, it's pretty exciting.

Lisa Young: Well, that's great. Thank you so much. All right, so then where can our listeners learn more? Is there any follow-up activities that you would recommend?

Sean Sweeney: In addition to the NIST CSF website, there's the site for that C^3 CQ program and there's also the crosswalk that I mentioned is actually on U.S. CERT's website. And I think that will really -- for security people out there that are used to working with these other frameworks and control groups that'll really drive the message home of how the CSF fits into the larger picture.

Lisa Young: Thank you so much. So, Sean, is there anything else you want to tell our listeners before we close out the conversation today?

Sean Sweeney: No. Just that I highly encourage people to -- even if you're working with something else, take a look at the CSF. See if you can make use of it. It's not the most time-consuming of exercises compared to a lot of the other work we do in security. And most importantly if you have comments -- and I'll be a salesperson for NIST for a second -- if you have comments and feedback, get that to NIST, because they're really looking for that. So and that's about all I got to say on it.

Lisa Young: Well, thank you so much.