

Framework in Focus: Karen Ribble Spring 2022 (publish date: April 2022)

This issue's interview is with Karen Ribble, IT Project Manager at Augusta University Health. Ms. Ribble shares about managing projects in the health care sector, working with cybersecurity, and the importance of transferable skills.

Interview Full Transcript:

KAREN WETZEL: Hello. My name is Karen Wetzel, and I'm manager of the NIST framework at the National Initiative for Cybersecurity Education at NIST, or NICE. The NICE Cybersecurity Workforce Framework, published as NIST Special Publication 800-181, establishes a taxonomy and common lexicon used to describe cybersecurity work. The NICE framework is intended to be applied in the private, public, and academic sectors. In this edition of the NICE e-newsletters—e-newsletter series, *Framework in Focus*, it is my pleasure to speak with Karen Ribble who is information technology project manager at Augustus [sic] University Health. Karen, thank you so much for letting us learn more about your career pathway, understand the NICE framework from your lens, and learn about someone who is performing cybersecurity work.

KAREN RIBBLE: Thank you.

KAREN WETZEL: So I have a few questions for you. We'll just get started—jump in with the first one—to just start off by explaining your role and responsibilities as information technology project manager at Augusta.

KAREN RIBBLE: Yeah. So as a IT project manager I lead a project team of various stakeholders in some type of technology that's used in health care. It can be anything from a server upgrade to a new application to an innovative project or new medical device, and as a project manager leading that team it's really about kind of measuring—when you think of project management there's different levels of risk that you need to address, there's your tasks and activities on getting you to the final product or final G date, complete date, for whatever the technology is.

KAREN WETZEL: Well I—sorry, go ahead.

KAREN RIBBLE: And it may involve procurement, it may involve performance, process improvement of workflows, evaluating the existing workflows, and really kind of also looking at those processes and functions, and how can we make sure that they're secure and working appropriately for the provider or the health care worker.

KAREN WETZEL: You mentioned you're leading a team, so can you describe a little bit more about that team and the types of roles that they fill?

KAREN RIBBLE: Yeah. So from a project management team there may be a varied group of individuals that make up that team. It may be the actual end user who may be a physician or a nurse, but it may also be the technical folks as well that are really in the details of IT. It may be someone in our data center, it may be also we have data center analysts, we have our systems admins that I work with on some of our teams, and in addition too we have a cybersecurity engineering group that I may need to tap into and bring in depending on the project itself and what those deliverables are.

KAREN WETZEL: If you could talk a little bit more about that cybersecurity engineering group, of course our listeners are going to be mostly interested in that. How do those engagements happen? Are they a regular part of every project that you work on, or how do you know when to reach out to them?

KAREN RIBBLE: Yeah, and that's a great question, especially because of cybersecurity and health care, we are kind of navigating and trying different types of engagement with cybersecurity and health care. In some cases we include a cybersecurity engineer on every architecture review team, and sometimes as a project manager I may be tasked to work with an architecture review team which really is made up of more of the technical folks, and we always have security to basically point out any areas of remediation, identify areas of risk, and what sort of adjustments do we need to make, make sure that what product we're implementing is secure, and I've got a great example of one area.

In project management, in IT, we have different types of projects, but we had an application that we were delivering—a new application that impacted our radiology group—and in addressing some new enhancements that we wanted to implement for the patient to enter information, we brought in our security analyst to kind of review and work with the vendor on identifying some of those areas of risk, and could we modify the product to be more secure, and this vendor particularly was very open to making those changes. So we pivoted, and it delayed the project a little bit but wanted to make sure that it will be a secure environment for the patients, and that we're protecting patient data.

KAREN WETZEL: It's really that sort of security by design approach versus trying to load it in at the back end--

KAREN RIBBLE: Absolutely.

KAREN WETZEL: Great. Are you finding that there are some types of cybersecurity issues that come up often? Is there any top ones, things that are at top of mind in your work?

KAREN RIBBLE: I think especially for health care, some of the areas that—with every project that we've been implementing—is making sure that we have that secure login and credentialing, that we make sure that we use active directory in any application, so moving toward one unique login and password for our users but at the same time making sure that we maintain that level of access for that particular user.

One thing that we've been hearing in the news is especially—and I get this just from my bank account—implementing multifactor authentication with any of your applications, and that's one area that, you know, again some of our developers and software developers haven't moved to that. So we definitely need to work with those vendors to kind of modify so that we can have it more secure, but those are some basics on the local generic logins. We avoid doing that, and some vendors automatically do that.

The one thing that I think especially that COVID has shown is so much work is being done remote, and one of the areas that we've had to address is a lot of the vendors maybe in the past had come onsite for a go live for an application and a new project whereas now they're doing remote. Well then that means we're asking them to have a secure VPN, secure access remotely, and so those are some of the issues that I know our cybersecurity team has developed policies and procedures around that to make sure that—to give you an example, one of the vendors that we utilized, their programmer was in another country. So now even though the contract is with the vendor, the workaround for that situation is the programmer who was in a different country needed to VPN internally to someplace in U.S. before we would give them access.

So those are just similar things that come up, especially with the remote. It's a great opportunity, it's a great benefit for those in the technology field, but it also provides additional risk in the way of cybersecurity.

KAREN WETZEL: Well, in health care it's got to introduce a lot of complexity that other sectors may not experience. It's even just some of the things that you described about different kinds of access and who might need that access, it may vary, it may be not as—you have to really account for a lot of risk that maybe others don't have to account for. I know that you've been in this role since, I believe, end of 2020. So have you always been in health care? What brought to this field--

KAREN RIBBLE: No, I've—Yeah, yeah. It's I have always been in some sort of academic environment, either college or K through 12, and I was on the university side, the academic side, and worked with setting up our cybersecurity pathways and some of our cybersecurity outreach programs, and I got very interested in our GenCyber camps at the university, it deployed Girls Go Cyber, Girls Who Code. There's not a lot of women in technology, and I know through my career that's always been the case, but I've enjoyed being a mentor, and being involved and engaged in that aspect, but then I started thinking ahead. I guess the university also is a medical institution, a teaching medical hospital, and we had done some stakeholder groups, engagement groups, internally on cybersecurity in areas that we could strengthen, and I was interested in making that pivot.

So after 25 years I went back to school, I got my master's degree in information security management, and there was a strand for health care security IT, and I went that path, and that really is what helped springboard me into the position I'm in now—hospital side as a project manager, and I have my certification in project management—but it helps to have that

cybersecurity knowledge especially when it involves the health care IT and the health care environment.

KAREN WETZEL: There's so many questions I want to follow up with there, and I'll just chose one. So one, I'll go with the certification degree question I have. One of the things that we've been looking at is how do we expand the pipeline, for a lot of the reason you described, diversity, need for cybersecurity people, staff? There's so many reasons why, and so a question that comes up oftentimes is are there ways to join in the field that aren't always through these traditional degrees and certifications? You've just described that you did take that path, but at the same time it sounds like your experience in cybersecurity was brought to that, and maybe the other ones were supplementing. What are your thoughts when it comes to these pathways and the best way to go?

KAREN RIBBLE: Yeah. I don't think there's really one size fits all. I really don't, and I know what our organization is trying to do in the IT environment is they're trying to encourage us to continue to look at additional learning and additional certification, and so while some employers may require a college degree or an academic degree, I think there's also a trend in looking at well what more are you doing in staying current, and I haven't completed it, but Security+ is one of those areas for certification. It's one of those I started and stopped, but I have it on one area to pursue, and I think that just demonstrates to your employer that extra level.

I know some of the students that I had mentored, it really depends on the student, and there are some great technical colleges that are offering some great programs, and I know from Augusta University they have a pipeline from the tech college right into the university. So I think it varies on it, but I think just like we're seeing a trend of not a lot of women in IT, I think because there's such a demand for IT and there's a shortage that some employers are getting creative, and I know some areas in health care are wanting employees to pursue additional certification.

I know internally our department has started inquiring on areas that we can pursue, and I think from a cybersecurity standpoint, I think if I was a young person just looking at the field, I think that every opportunity that they can take whether it's on the technical side, or some of these programs offer some certification online learning without going through an academic institution.

Those are some of the varies, and I'm referencing one of the high school girls that was in the Girls Who Code, she had done a couple of online programs to kind of pique her interest, and realized she wanted to do that, and I still keep in touch with her. She's now in her second year in college, and she's actually at Augusta University attending the cybersecurity program. So I think those are just what opportunities are out there. I think the young folks should certainly take advantage of it.

Now someone my age, you know, you're never too old to learn something new, and I think if you have that interest, I've always had an interest in information systems and processing. I may not have always liked the programming aspect of it, but I've had the analytical skills, the analytical and that troubleshooting of how can you use technology to improve a process. Think now with going back and getting additional knowledge is helpful in my job even today.

KAREN WETZEL: That's one of the things that, again, another area we've been focusing on is understanding that it's not just about that one pathway. There are so many ways of coming in and rescaling, upscaling, and definitely looking at where are people, you know, what kinds of qualifications people can bring that maybe weren't from that traditional four year computer science kind of degree, but as you've described it yourself, to be able to—I have an interest in this, I have some strengths that can be really put to use in this field. That's one of the things that we try to do with the NICE framework is show the variety of different kinds of roles there are in cybersecurity. So maybe going to that next, looking at the NICE cybersecurity framework, how do you see it being useful for people who are maybe looking at joining the field or even in the field now and maybe looking at different kinds of ways to engage with other cybersecurity roles? How do you see using it?

KAREN RIBBLE: I think especially with some of the partnerships that NICE and NIST have done with CyberSeek, and how you're able to look at those areas of the framework and look to see those careers that map to it, and just like I said, the programming aspect, I knew that I didn't want to go down that route, but I did have an interest and, again, pulling on what your strengths are. I think those are the tools that a lot of our young—anybody young, but even making a career change, to kind of look at taking those strengths or those areas that are in there. Like when I think of the project management, I kind of follow the oversee and govern part of cybersecurity, but there are so many other areas.

I've also thought about the auditing area, the risk management. That was one option that I was looking at too in health care, but I've landed in a great spot, and every day is different. There's challenges obviously with every job, but I think this is a great time that the work that's already been done so far that's helping to improve all those industries especially where I see in the health care arena.

KAREN WETZEL: We—with our latest revision—introduced competency areas as well, and I could see how someone who may not be a project manager as their job might still have need for some project manager expertise too, and so we're looking at competencies as a way of sort of framing those of I need to have some of this knowledge to be able to apply some of this knowledge in what I do even if it's not my primary job role.

KAREN RIBBLE: Right, right, and that's one thing I will say about Augusta University. One of the areas that they've just—the business school has added project management, and I know from the IT and some of the cybersecurity degree programs they've added that as an elective originally, but now they've kind of transitioned that it's part of every academic program from marketing to even in the accounting arena because project management is really used in so

many industries, but you don't necessarily have to be a PMP but in some cases you do need to lead a team or kind of identify a schedule and those milestones and get a completion date. So yeah, I think there's lots of progress moving forward in exactly what you were outlining there with the framework.

KAREN WETZEL: It's a lot like how we see the growing recognition for the need for professional skills, sort of those communication or--

KAREN RIBBLE: Communications, yep.

KAREN WETZEL: Right, yeah.

KAREN RIBBLE: Yeah, the soft skills. Those are so needed, but at the same time I know, you know, and I can see some of that approaching in health care with the various teams, we've got different strengths and different expertise, but I know from the cybersecurity standpoint when we talk about recruiting folks outside of the norm I think that diversity of thought is so important, just bringing a different perspective. I deal a lot with physicians and nurses, and sometimes because I'm not a nurse and I'm not a physician I can bring an idea, approach to them—because I'm thinking a little bit differently—with success, and I think the same has been true for cybersecurity for those nontraditional types that they recruit that you can offer that diversity.

KAREN WETZEL: Let's talk about that a little bit more. You mentioned the work that you had done with the GenCyber camps, the Girls Go Cyber, and Girls Who Code kind of work. Could you talk a little bit more about how you have worked in making sure that we are working in a place that's not only welcoming to a diverse group of people but also the value that—as you were touching on there—that it brings to our work.

KAREN RIBBLE: Yeah. I think the GenCyber and the ones that I mentioned before, Girls Who Code and the Girls Go Cyber, I think it helps bring girls to that idea, and I know I've seen it to some of the groups that I've worked with, they may not be programmed, or they may not have that self-confidence, or they've just watched too much stereotypes on T.V. that they think, oh, well I'm not good in math. Well math, that has nothing to do with it. You need to look at what your interest is and what your strengths and that motivation, and I will say the Girls Who Code it was an interesting group, you're working with high school girls. In some cases we need to expose cybersecurity and technology to some of those at a younger age, but I think by giving them those avenues of exposure and experience. The GenCyber camp, we've had some that come out of that that love it. They might not necessarily have chosen that as a career path, but they've learned the importance of security, and they've changed their behavior. That's a plus. Of course--

KAREN WETZEL: And that's huge. Absolutely.

KAREN RIBBLE: Yeah, that's huge. Of course we do want them to be engaged and go, "Yes, we're going in there as a profession," and we have those too. I think we definitely see that awareness, I think we still have a ways to go to break that stigma of well, you've got to be tech savvy to go into this field. Well, no you don't. You have to understand and comprehend certain things and articulate but you don't necessarily need to be in the weeds and the details.

KAREN WETZEL: And there are lots of different kinds of roles in cybersecurity. We have over 50 defined in our framework. So really understanding that it's not—I think a lot of times we are informed by mainstream media, and you look at T.V. shows, and you've got this one kind of cybersecurity image there, and that's T.V. and movies. There's lots of different kinds of work, and we really spend a lot of time with the NICE framework emphasizing that what we have is meant not only for those who are entirely in cybersecurity. It may be that cybersecurity professional, but really that cybersecurity is something that people need across an organization regardless of your role--

KAREN RIBBLE: Right, right. Yep.

KAREN WETZEL: I know those folks who do cybersecurity awareness out there are on our side here, but that's exactly it. It's understanding that every person needs to manage risk in their organization, and there are things that you could do and certainly, as you mentioned, with our banks. We all know that from our own personal experiences as well—

KAREN RIBBLE: Right.

KAREN WETZEL: —the apps on our phones and the two factor authentication.

KAREN RIBBLE: Right, right.

KAREN WETZEL: Yep.

KAREN RIBBLE: Absolutely.

KAREN WETZEL: So you mentioned a little bit, but to go back to it, about keeping your skills sharp and current. What are ways to do that? Obviously you're lucky I think where you are. There are a lot of programs available to you, but what are some other ways that you might keep up with what's important now?

KAREN RIBBLE: Well, I think especially with everything electronic and available online, I subscribe to several key periodicals and newsletters that are in the various fields. I stay current with the NIST publications. I login to ISACA the *SmartBrief* on cybersecurity. There's one that I register for on health care that I get daily briefs, and they're really more, and I guess they're not necessarily skills, but in some of those newsletters they may offer a one hour on a new topic, or they may offer a series, and so I always try to—when I come up to one of those periodicals and newsletters—I always try to register for those info, and I know like there's one

through a health care organization that they'll send periodic—even through some of the online learning management where if you don't make the webinar then you can login and view it later. I've done that a few times. I've done that even on my lunch hour where I'll login to a one hour webinar of an area, and from a health care perspective I know I like to stay current on changes in HIPAA and anything that—what other organizations are doing. I think it's always good to stay current in that aspect, and of course conferences that come in the area.

KAREN WETZEL: I think during all the interviews I've done since I've joined here at NICE, the one common thing that I hear when asking this question is about the community, about how really it's you may be on a team of one at your organization but understanding that there is a broad cybersecurity community out there that you can engage with—

KAREN RIBBLE: Oh absolutely. Yep.

KAREN WETZEL: —examples that you just gave, and I like that you also shared some of the, you know, depending on what sector you're in or what kind of work you're in, there are ways to expand that beyond just this straightforward, you know, it says cyber in the title. What are those other areas that you might want to also go to and where there are these conversations taking place as well?

KAREN RIBBLE: Oh yeah, and I know from the health care, from our institution, we were active in a project for cybersecurity and identifying those areas that we needed to improve, and our chief information security officer, I've been pinging her saying, "We need to have a white paper out of this." We need to get on the lecture circuit or the conference circuit because I think there's some applications that we, you know, what we've learned from areas to improve on can also help another organization maybe smaller than us but that, like you say, don't have the resources, but you can at least offer that. So you're definitely—you hit it, the cybersecurity community, any ways that you can kind of tap into that, absolutely.

KAREN WETZEL: I love that you're thinking of it from a giving back to, about what can we share back, how can we do it? I think that's a really important aspect of understanding what have others done, and there's always something that you're working on I'm sure that somebody else hasn't quite figured out.

KAREN RIBBLE: Yes. Yes. No need to invent the wheel. Let's share, and how can we solve this problem together and, yeah, I've always been thinking ahead in that aspect. So even though I've pivoted to health care I still think that with how can we improve or help others improve?

KAREN WETZEL: I love that, and it's a great way of starting to get other people to start to know, "Oh wait, you know what? Karen might have something on this," and then be able to share back to like, "Hey, we followed that, but we made this adjustment, have you thought about that?" It really keeps growing.

KAREN RIBBLE: Yeah.

KAREN WETZEL: So I have just a couple more questions. One is what do you enjoy most about the work that you do? What gets you up in the morning?

KAREN RIBBLE: You know, the thing that I really, really enjoy is every day is different, but I love that I'm able to engage with different groups, and I'm involved in one project it's got, oh, so many—it's got probably 50 people on it and they're all physicians but they all are wanting to improve the patient's view of cancer, and it's all related to the clinical trials and what they're doing to support their clinical trials, and I think, wow! I don't understand all of it, but I'm just amazed that I'll be in a room and there's these, you know, all the brain power, and yet we're implementing something, a tool that they can use, and we're using multifactor authentication, to improve research and improve the patient experience. I think that's what's exciting.

KAREN WETZEL: It's that big picture of understanding that what we're doing in cybersecurity and with technology is really having an impact, you know, what is the end result, how does it improve--

KAREN RIBBLE: Absolutely, yeah, and that's one thing that I think I've even shared with some of my colleagues here that's like just the amazing aspect how technology is used everywhere and yet, especially in health care, all the various levels that we're touching in that big picture like you said that, wow! We're using technology in the hospital to deliver meals to a patient who's in there to be treated. I mean that's just amazing.

KAREN WETZEL: And I'm going to have to ask you at some point about that another time.

KAREN RIBBLE: Yes.

KAREN WETZEL: I've not even seen that. That's amazing.

KAREN RIBBLE: Yeah.

KAREN WETZEL: Yeah, it really is, and making sure we're doing so in a way that's going to mitigate risks and doing so effectively, it's so important.

KAREN RIBBLE: Yes.

KAREN WETZEL: The last question then, so if you were able to give advice to someone who's considering a career in this field, maybe wants to follow your footsteps and do something with project management, what would your advice be?

KAREN RIBBLE: Gosh. There's so many areas, but I think getting into your community and looking at ways, if you have an interest, there are so many organizations that may not have that particular role, but if you could take on an effort for them to just get in the door and have that interest. I think that would be beneficial, and I think also, I say this with any of the students I mentor, just to have an open mind of what areas that you want to choose your career but

acknowledging it may not be the same career 10 or 20 years, but yet if you have certain skills, just like you can pivot to another industry and take those skills with you. I think that's, yeah.

KAREN WETZEL: You were saying before that one of the things you like is how it can be different every day, and I think that's again something I've heard before. It's something I like about my job, but at the same time it brings with it the other aspect that this is not a field that's going to stay the same. You're not going to start this job and then five years later you're doing the exact thing.

KAREN RIBBLE: Right.

KAREN WETZEL: So understanding how do you actively maybe manage your career or where you want to go, or one thing I had heard once was someone saying, "Keeping an eye out at what other people are doing," like things that they're doing that you might be interested in, and sending them a note and saying, "Hey, I'd like to talk to you about your job," or, "Hey, can you share with me a little bit more," or in your own organization saying, "Hey, maybe I could spend an afternoon with them and find out more about what they're doing," and exactly, always sort of keeping your eyes open.

KAREN RIBBLE: Yeah, and I think that's probably a skillset that everyone needs a little improvement on, the networking, just networking with others and joining those different organizations, but I was on the university side, and I was interested in health care, and I wasn't quite sure where I wanted to pivot to but I actually took a semester off to finish my degree, but I worked alongside a health care management professor just to learn a little bit about health care and what she was doing, and that's when I realized, yeah, I need to go there, I need to go that direction.

KAREN WETZEL: Well, and that's great. It gives you an opportunity to find out is that actually where you want to go.

KAREN RIBBLE: Right.

KAREN WETZEL: It's getting your toes wet without having to dive in all the way.

KAREN RIBBLE: Right, right.

KAREN WETZEL: That's a good idea.

KAREN RIBBLE: Right.

KAREN WETZEL: Well, thank you so much, Karen, for your time today. I really appreciate it and enjoyed this conversation.

KAREN RIBBLE: Oh yeah. This has been fun, and I'm glad to have shared my information for anyone who might be interested in the IT project management, but of course in the health care arena as well.

KAREN WETZEL: Great. Thanks so much and hope to see you again soon.

KAREN RIBBLE: Okay. Thanks.

[End of recorded session.]