Framework in Focus: Leeza Garber

Winter 2020 (publish date: January 2021)

Leeza Garber is an attorney who specializes in privacy and cybersecurity law, a corporate keynote speaker and consultant offering problem-solving sessions related to cybersecurity, and a co-founder of Can. Trust. Will., a best hiring practices LLC focused on cybersecurity hiring. In addition, Ms. Garber teaches Internet Law at The Wharton School at the University of Pennsylvania and is an adjunct professor at Drexel University's Thomas R. Kline School of Law, Drexel Law School where she teaches Information Privacy Law.

Interview Transcript:

My name is Karen Wetzel. I am manager of the NICE Framework with NICE, the National Initiative for Cybersecurity Education at NIST. The Workforce Framework for Cybersecurity or NIST Special Publication 800-181, is a fundamental reference for describing and sharing information about cybersecurity work in the form of tasks, statements, and work roles to perform those tasks. It establishes a taxonomy and common lexicon that describes cybersecurity work and workers. I am happy to introduce today, Leeza Garber, a consultant and adjunct professor for today's Framework in Focus. Leeza, could you tell us a little bit more about yourself?

Leeza: Hi Karen, great to be on with you today. I am a consultant and I am also an attorney. I specialize in privacy and cybersecurity law. I'm an independent consultant where I offer corporate speaking engagements and problem-solving sessions related to cybersecurity. I am also a consultant with Can. Trust. Will. LLC which is a best hiring practices LLC focused on cybersecurity hiring. Additionally, I am an adjunct professor at Drexel Law School in Philadelphia where I teach information privacy and I'm also teaching internet law at the Wharton School at the University of Pennsylvania also in Philadelphia.

Karen: Sounds like you have a full plate. Thank you so much for that introduction. I wonder if we can tease into some of the roles you play starting with your roles and responsibilities as an attorney specializing in cybersecurity and privacy law. Can you explain a little bit more about what that means?

Leeza: In general attorneys are trusted advisors, that's the role they fulfill whether they are litigators or performing contract work. In cybersecurity and privacy, litigators deal with active cases on data breaches or standards in cybersecurity and then the flip side is the contract work that might be dealing with insurance, cybersecurity insurance, different policies, best practices and procedures, legal standards, privacy policies, all of those things. For me, I got to deal with quite a bit of both and I also was an in-house attorney for a cybersecurity and digital forensics firm for a few years and now I've moved on to do more consulting work, educational work, and work related to how to best hire for cybersecurity and that's with Can. Trust. Will.

Karen: Thank you so much for that. With that background how do you translate that into consulting? What made you move into that area?

Leeza: I think lawyers are a natural fit for consultants because we are analytically natured. We know how to communicate with our clients if you want to be successful, and we deal with really complicated problems. I think it’s a really nice fit to be a consultant in many different fields. For me I was passionate about tech, cybersecurity, and privacy, and that led me to think there are so many things I can do within this field. As a consultant I felt more open to pursue many of my passions related to cybersecurity versus just sticking with either litigation or contract work and consider myself a trusted advisor for corporations at many different levels and in many different fields. Cybersecurity, as you and the listeners know, plays a part in every single one. I think it’s really benefited me and it’s also a way to pursue my academic interests in teaching law students and undergrad the important pieces of information privacy and internet law.

Karen: That’s got to be rewarding. You’ve done so many different kinds of roles, and have worked with a lot of different kinds of people as well, can you share a little bit about the kinds of roles of people you’ve worked with both as an attorney and in your roles as a consultant?

Leeza: It’s helpful to give a little bit of background as to how I actually got into this. I think it helps shape the types of people and the work roles I’ve worked with as well. It really started in law school. I had a wonderful privacy law professor at Penn Law, Anita Allen, who is a renowned scholar in the field. She calls herself grandmother privacy and that really instigated my interest in it. I started out as a litigator in a completely unrelated field but then moved into technology. I was fortunate enough to complete a business and public policy cert at Wharton when I was at Penn Law. I had meetings with people that were app developers. This dates to quite a few years ago but it really helped me get connected in the tech space. After working as a litigator and then doing contract work in the privacy world I moved in-house and that’s where I really got to see the general cybersecurity and privacy issues that in-house lawyers encounter on a daily basis and the types of knowledge they’re expected to have in terms of cybersecurity and privacy. I think obviously larger companies are now getting more specific privacy related roles and even cybersecurity legal roles but even just a few years ago it looked very different. Now I really do get to use my legal background to problem solve and I really see lawyers getting into the NICE Framework category of obviously legal and advocacy and that’s one of the specialties in work roles. I think it’s so many other categories under the Oversee and Govern section. I actually have the NICE Framework pulled up here. I think within Oversee and Govern lawyers really need to work with the training education and awareness team, they need to work with the cybersecurity management team, the strategic planning and policy team, and the executive cyber leadership, because lawyers really need to be involved at the get go. They help to bake in best practices and lawyers are also forced to be able to look into the future and see how the law is evolving, especially related to privacy laws. Also, cybersecurity standards like NIST and NICE helps remind us these are changing, and they have to evolve with the technology. It’s also understanding what the FTC is doing, how they are responding to different data breaches and privacy implications. Lawyering really helps every aspect within a corporation stay up to date. I think they’re vital to so many work roles especially within the NICE Framework.

Karen: That sounds like a really interesting approach. Just what you’ve described, it’s great to be able to work with so many different kinds of roles and to be able to see how your expertise can really help the field with those different kinds of roles. Thank you for sharing that.

Leeza: I’ll add one piece. When I look at the NICE workforce categories I obviously mention Oversee and Govern but I think lawyers can also be helpful in the investigative teams because when they’re looking into cybersecurity events or criminal activity related to IT I think lawyers can be extremely helpful in helping to parse a part of what kind of evidence is needed, what the investigation should look like, what it actually needs to cover, and so I think lawyers working in cybersecurity, we don't have to be super 'techies' but there has to be a level of understanding to appreciate how to be the most helpful.

Karen: I'm sure things like communication and being able to work with teams and building those relationships with folks so that they know to come to you and know that you can help advise them as they work in those different areas.

Leeza: To not be a scary lawyer but to be someone that is approachable that wants to be a problem solver, that wants to be part of a team, it's inherently important and I think it's something that the NICE Framework does really well - emphasizing that regardless of these separate work roles they're all intertwined within the larger community and that is vital for cybersecurity.

Karen: That's excellent. I was just thinking what a great soundbite that was. We just finished up our NICE Conference for this year and you had presented on putting the NICE Framework to work hiring cybersecurity talent that is highly able and not just highly skilled. I wonder if you can share a little bit more about that distinction you made there and how the Framework can be used as a guide in one's career?

Leeza: The presentation I had been very fortunate to give at the conference was actually alongside my business partner for Can Trust Will, Jack Olsen, who is a former FBI agent and specializes in leadership. He actually put in place many of the leadership processes that are used in the FBI today. What we came up with was this idea that yes, you can have someone that is highly able, but they might not be highly skilled and vice versa. There may be someone who is very highly skilled but not able and the fundamental difference here is what the person *can* do and what they actually *will* do. Particularly when under stress. There may be somebody who is very highly capable, highly experienced, highly educated, and has all of the certs you can possibly count, but they might freeze in crisis. Not all of them do obviously but it can happen. Someone who may not have that really highly educated background, all that experience, may be great in a crisis. Not because they have some remarkable depth of understanding but because they can manage in a crisis, they can handle that kind of stress. The point of this presentation was to understand that the key isn't to align a hiring process for cybersecurity just to look for highly capable people, people that have all of the bells and whistles in terms of cyber education, but the point is to really understand what you need and that is something obviously that the NICE Framework details thoroughly in terms of what kind of work roles exist, and it provides that fundamental ground work for understanding what your company needs. The question then becomes, as you move forward, and it gets more complicated, what you actually need and how do you filter for what you need in terms of a hiring process? We argue that you first filter for *can*, the capabilities, and then you filter for *will*, what a person actually will do in a certain situation. We get questions all the time and got phenomenal questions during the NICE presentation during the conference such as how do you know whether somebody's going to do, what kinds of questions can you ask, and it comes down to a behavioral interview. The point is, timeframes are real, stress is real, decision making is necessary every minute of every day, and that can interfere with what a person will do when they actually show up for work. When you talk about highly able versus highly skilled the NICE Framework defines abilities and skills. The Framework defines ability as confidence, perform observable behavior, and skill is defined as an observable confidence to perform a learned psycho motor act and it goes into more depth. In this way you can use the NICE Framework for strategic workforce planning and hiring, and obviously there is a discussion on KSAs in many government entities and the question then becomes what's next and that is understanding the layer of difference again between *can* and *will*. We're hiring people in cybersecurity; we're not hiring machines. One of the points I love from the NICE Framework is, and I'll quote it "A current employee has existing relationships, institutional knowledge, and organizational experience that is hard to replace. Refilling a position after an employee leaves may bring new advertising and hiring costs, expenses for training, diminished productivity, and reduced morale." It goes to show how important it is when you find, the right fit, but it's so much more because it's understanding the basic framework that NICE offers. I say basic, tongue and cheek, because its heavily complicated in terms of everything that's necessary for a cybersecurity workforce. It's understanding what your company actually needs and then what the person is, that your company actually needs to fulfill that role. It's how to lay the NICE Framework over human teams.

Karen: I can see from your descriptions there, not only is it then something that obviously an employer would be looking at, and as you pointed out, comes into the hiring process, but as someone who's in that field to understand that as well and how they might fill these roles and then be able to gauge their capabilities when it comes to both skills and abilities. Following on that, what kinds of cybersecurity jobs do you think are the most difficult to fill? Do you think they will change in the near future or do you think this is the job that is always the hard one and will probably be like that going forth?

Leeza: I think we can look at some of the statistics related to cybersecurity and they are pretty dismal. CyberSeek, which is the fabulous project that NICE supports which focuses on supply and demand in terms of the U.S. cybersecurity job market, highlighted that there were approximately half a million open cybersecurity job listings from June 2019 through May 2020. The Bureau of Labor statistics reports that the job market for Infosec Analyst is growing at a rate of 32%. Harvard Business Review says the majority of CISOs around the world are worried about the cybersecurity skills gap. There are so many unfilled positions related to cybersecurity. IBM says cybersecurity jobs take longer to fill; they take 20% longer than typical IT roles. It's a problem. I think that it's because we're approaching cybersecurity job applicant pools in the wrong way, but I also think it's not just one specific job, one specific role that's tough to fill. I think technically we could look at them all as tough to fill. The problem is that raw skillset, the *can*, can be complex and expensive. To take someone who might be suitable and then train them up, give them the right tools, give them all the things they need to get that job done. In essence, we still have to go back to *can* and *will*. Once we separate the actual skills versus abilities, we're in a much better place to assess what kind of person we need in a certain job role. I think it requires not just an audit of what your organization currently has in terms of cybersecurity related to the NICE Framework but what is missing according to the terms in the NICE Framework, what you have in house, and what you have outsourced. It's also a deeper dive into behavior and that's the real question in terms of how you find that right person for your team. It doesn't matter whether you have two people or two hundred thousand. It's really understanding the ability to have a team that can work together and as we all know from cybersecurity that's absolutely vital. It's a question of finding, hiring, and keeping the right employees and for cyber it's always going to be difficult because they're in-demand and when you appeal to security talent it doesn't matter if you have a really incredible paycheck offering, or benefits package, or a pool table in the office, there is so much more. It's really about the culture of your company and finding the person who can get the job done and will get it done.

Karen: Those are great insights and I can see too, with this field in particular, we're always saying that technology is changing quickly, its growing, but I think in cybersecurity we're seeing that growth in perhaps more so than in other areas. You need to constantly reskill and look in and apply new skills so finding someone who is a continuous learner and being able to support that in your organization I think will be really important.

Leeza: That's such a good point and it's something we've heard over and over again at Can. Trust. Will. and also, I should mention my business partner and I have a manuscript for a book coming out hopefully next year on cybersecurity hiring. We got to interview quite a few folks related to cybersecurity hiring and in the cybersecurity field including Rodney Petersen, the Director of NICE, who I'd love to quote here moving forward in the interview. Really there are so many open positions and they are only going to grow because more organizations are going to realize that they need more people in cybersecurity, there are new roles that are going to emerge, so its staying on top of things and being able to come back to a great resource like the NICE Framework helps to make people feel less overwhelmed. Especially for a field like cybersecurity which is constantly evolving.

Karen: We are updating our Framework it should be a new release should be out in just about a weeks' time. It's about making it more flexible, more agile, and modular and interoperable, and so looking at things like those tasks, skills, and knowledge, but also adding to it competencies as a different way that the Framework can be applied because we're hearing that as well from employers the need to assess from a slightly different angle than just the certifications alone which leads me to my next question. How important is it to have a cybersecurity related academic degree or certification in this field and how does that relate to competencies?

Leeza: This is a point that is definitely addressed heavily in the book because we see folks from small cybersecurity start-ups to large cybersecurity companies that are offering their services as outsourced, and large financial institutions, large health care institutions, that have them in-house and also government institutions that are saying our standards need to change a bit because we seem to be looking for candidates that don't actually exist; that don't have all of the academic degrees we want, don't have all the certs. They're not coming super prepared for a specific role and I love this quote we got from Rodney Petersen, the Director of NICE, when we were interviewing him for our book, he said "position descriptions are over spect'd and the number of open jobs and certification requirements often exceed the number of people available who even hold them in the universe." I thought that was illustrative of some of the problems for security spaces in the coming future, which is yes, there are not enough people necessarily but we may not be looking in the right places either. I'm an educator in cybersecurity and I fully believe in many of the academic programs that are offered in the field. I think if you learn that way it can be phenomenal. Certifications are also a fantastic opportunity as long as you choose the right ones. I think there is quite a bit of competitions in the field. There are a couple of foundational companies, non-profits, that we can trust but in essence competencies can be obtained in many ways. That's something we continue to see in cybersecurity. It's certainly dependent on the specific role you are looking for or the responsibility you are looking to have but competency can come from experience and that can be from work or it could be personal. Companies may really want the man or woman who's been hacking away at systems in their basement, the stereotypical hacker type who really learned on their own versus somebody who comes in from an academic position and really understands the history of the systems, how they function, and everything else. There is also certifications and training which can happen pre or post hire. That's something in interviews I saw becoming more popular, that you could take someone, and if you know they are right for you because they have those abilities, the will, the quote unquote the *will* of getting things done in your office on your cybersecurity team; train them up after, give them the certs after, give them the opportunity to gain the experience on the job. I think academic degrees are still vitally important for people who are able to learn that way and they can be a game changer because many of the requisite degrees we see in cybersecurity job descriptions make sense based of the defined responsibilities. I think that is something we can look to the NICE Framework on, but I think it also depends on how mature a company's cybersecurity team is and how senior the role is that the education becomes more and more important. In essence, it depends on what corelates to success for a specific role for your specific organization. That comes back to understanding what you need and that comes back to the NICE Framework.

Karen: It does seem like it is all about intentionality as people are looking at creating those job descriptions that they're not relying, necessarily, on the canned description that was already put out maybe a couple of years ago. We talked about continuous learning from the employee learner side but I think perhaps on the other side of things, of the employer side, the constant re-assessing and understanding what your current needs are and anticipating future needs to so you aren't just relying on "well you put this out before so I'm sure it's still fine. "

Karen: It's true. Your word on intentionality is on point because yes, it may seem more labor intensive and more of an obligation, more responsibility, to be intentional about those job descriptions and updating them and making sure your team continues to get the right training. In the end it's just like data breaches, you put in that effort up front and be proactive, you're going to be better off down the line. The preventative measures are always better, and I think in terms of being intentional and trying to say we can't stay ahead of the curve, but we can try to stay on top of it, that's the way to go.

Karen: And certainly not behind it. Turning back to you Leeza, how do you yourself keep your skills sharp and current? It sounds like at least with your work in hiring a lot of it might be reaching out to others in the field, but you let me know.

Leeza: I'm very fortunate because my job roles now force me to stay current. There are so many amazing resources first of all. We look at publications put out by NIST and NICE. We look at the SANS Institute, the International Association of Privacy Professionals (IAPP), academic institutions, and white papers. For me it's also chatting with my colleagues, especially in tangential areas like crypto currency, cellular text, artificial intelligence, and the internet of things. I think all of these areas that are fundamentally related to cybersecurity help teach us what's coming up ahead of the curve. I've actually been asked to host a show for the American Bar Association Automobile Litigation Committee. That's based on automotive litigation related to self-driving cars and AI in automobiles and the upcoming technical issues related to automobiles. That is something completely different, but it's all related to cybersecurity and then we think about what kind of work roles are necessary for these areas. In addition to that I consult with a broad range of clients. This forces me to stay extremely current. Teaching allows me the opportunity to look at new scholarship on new uses of existing text, upcoming inventions, and additionally I also commentary for national news on cybersecurity privacy and social media. I have to stay on top of everything that is breaking news in this field. I think because of the roles I've chosen I have to stay on top of these things and fortunately in this area we have phenomenal webinars that are offered, especially during the pandemic we can get so many of these resources online, and I think NICE did a phenomenal job with its conference this year in terms of bringing amazing speakers in to talk about so many of these issues.

Karen: It's one of those things in this field of cybersecurity is just how great the community is. Like you said there are so many organizations that are putting out amazing resources. We all have the opportunity to keep apprised of happenings in things like newsletters, articles, webinars, and even online conferences now. There is no shortage of information out there so being able to take advantage of that is great. There is no such thing as resting on laurels in this field either.

Leeza: It's so true. The only thing we have to recognize is time management because sometimes you can find something really interesting about this super small part of a crypto currency cave or for me, recently, it was a bio metric case and then all of the sudden you are down a rabbit hole. It's time management and being able to understand we can't know everything at once, but we need to stay up to date on everything. What's the latest FCC decision, what's the latest law coming out of California related to privacy and cyber so that's really where, as attorney's we have to look.

Karen: My next question is about diversity and how does diversity play into your work and what advice you might have for organizations who are looking to broaden their workforce diversity? I know this came up a little bit earlier when we were talking about hiring and degrees and different kinds of roads but what advice do you have in this area?

Leeza: I love talking about diversity because I'm a woman in a pretty male dominated field whether you pick law or tech. Coming out of law school, I was one of very few women in my legal offices moving through jobs. Then I realized privacy tended to attract quite a few women for some reason and in cybersecurity I see the numbers growing but the most important piece to remember about workforce diversity is that your team will fail if it is not diverse, plain and simple, in cybersecurity especially. When we talk about diversity and inclusion its really diversity versus uniformity. Diversity is a moral imperative for sure, but it is so much more than that. Diversity is a fundamental part of an effective cybersecurity team and the analogy my writing partner for the book loves to use is a soccer field. If you don't count diversity in a cybersecurity team it's the same as putting eleven goalies in a soccer field. You need those broad ranges of perspectives on your cybersecurity team because it's a compliance issue, it's a performance issue. Cybersecurity has to be driven by creativity. Its problem solving, its being able to work quickly under pressure, and a uniformed team kills creativity. Diverse teams perform better because diverse perspectives drive creativity and diverse cybersecurity teams beat uniform cybersecurity teams every time and it's something that we found in many of the interviews we had with major cybersecurity professionals including CISOs and CIOs. I love to quote statistics that most recently the percentage of women in cybersecurity is still about 24% and that's dismal if you are talking about gender. Obviously, diversity applies across every other field you can imagine but we have to remember talent is equally distributed among the population. We need to represent all of these groups in terms of diversity and in cybersecurity where we're dealing with really complicated problems. We need diverse talent to attack a problem from their multiple ranges of perspectives. Diversity is a must-have and I think once we look at it as not a moral imperative or something that we have to do because HR says so, we have to do it because it will lead to our success plain and simple. Once we start looking at it in a different way, I think it helps broaden applicant pools as well as candidate pools. It comes back to *can* and *will* capabilities versus abilities. When you're looking at someone who may be a great person to deal with stress, to deal with these really hot crisis situations, they may not have that exact education or the couple of certificates you have in your job description that, as you mentioned earlier, might have been last updated three years ago but you see through a behavioral interview that this is how they interact, this is what we know about too when they come into work and are hit with something very stressful, let's train them up. Let's open our applicant pool, let's open our candidate pool, and by doing so we'll also assist in diversity which as I said before is vital for success in cybersecurity.

Karen: I absolutely love the statement you made that if we don't have diversity, we have uniformity. It's not something I've heard before and it seems, so, like why haven't I heard that before it's such a great explanation of how important it is, especially, as how you point out, in cybersecurity. It's a field where you need to be creative, you need to think from different perspectives, and having that diversity of thoughts is one where you really need to do that. Do you have any suggestions to organizations who are looking to broaden that? You mention a little bit about perhaps being more flexible with the job descriptions and all? Any other suggestions you might have where you've seen, or any anecdotes you might be able to share, of how people have improved their diversity?

Leeza: I think it's also looking in places you might not initially suspect for good candidates. I think what's so important for hiring managers, and even if you don't have a hiring management position just somebody that is in charge of cybersecurity or even just IT within a team, being aware of what the academic institutions around you are doing. I know that at Drexel which has a phenomenal cybersecurity program there are partnerships with different companies where students can come in and intern and they end up getting hired. I think when you see the types of students that are really interested in the field, they may not be techies either and I actually had a phenomenal experience with a former student of mine in my Drexel law class who was actually a management reporting analyst for a bank where he reported to accounting risk and operations, and then she moved on to the infosec team developing response and business continuity plans. Now she's actually an information security analyst. I think you can look to starting positions in terms of what the universities around you have graduates in and then also look at internally maybe of someone who can move laterally that we weren't thinking of before who offers the diversity and perspective and also actual diversity. I think it's about really where you look for candidates and then having more open parameters and that comes back to re-assessing the jobs you need filled, what the people need to be able to do, and what they will do in the role.

Karen: I love the advice about the lateral move and looking internally too because not only does that, as you say, sort of broaden your pool, but it also offers a lot for your employees too. To be of the understanding that there may be additional opportunities or moves that someone can make in one's career.

Leeza: It's so true. I get calls from students all the time, either students that I have currently or that I used to have or that are referred to me because they want to work in cybersecurity. The question I get is well, how much tech do I really need to know? I'm coming at it, obviously I'm a lawyer, I'm not on the technical side, I can talk the talk. I have training in certain digital forensics technologies and I understand how to review incident response reports and all of those things but when it comes down to it I took one coding class in college and I would love to be able to do more in all of my free time. It's not happening right now; I'm getting a lot of my experience on the job. What I tell people is if you're going into it looking at a non-technical career, be open to learning the lingo, be open to maybe taking a coding course or a forensics course. You can still make that lateral move if you have an appreciation for risk if you have an appreciation for how these skills operate. One of the things I love about the NICE Framework is that it's coming at it from all angles. Yes, we need the techies who will handle incident response and who's going to handle the digital investigations and building firewalls, but we also need the person who's going to come in from a legal perspective or from a risk management perspective. There are so many ways into this field.

Karen: That's really great thank you so much. What do you enjoy most about the work you do?

Leeza: Honestly, I'm so passionate about this field I count my lucky stars every day to having ended up in cybersecurity and privacy. I think it's one of the most exciting fields to be able to work in as a lawyer and a consultant because it changes every single day. I think we're living on the cutting edge of this technology in terms of what's going to happen to consumers data, in terms of how we handle data breaches which are now part of our daily lives in terms of how we handle new types of threats. Honestly, I love every piece of my work and I think one of the most fulfilling pieces is getting to talk to students who are really intrigued by entering into a career in cybersecurity, and what's so fulfilling to me is that I can speak to experience from my Wharton class last semester where I had sixty undergraduates coming from all different kinds of backgrounds and all different kinds of majors interested in learning about internet law. A great bulk of the course was spent on cybersecurity and seeing the ability these students have and having them understand that they've grown up with this technology and they have something extremely valuable and significant to add to the discussion on policy, procedure, and the law, in terms of what happens with technology intertwining with humanity in the future. Being able to guide students and let them know about all the opportunities that are available in this field is something I absolutely adore and wouldn't trade for anything.

Karen: That sounds amazing and I think your students must be lucky to have you. When they do ask advice, what is that advice they typically ask of you? You mention, do I need to know coding, is there advice you typically give to those new students as they are entering in this field?

Leeza: I usually say get involved so I offer different organizations that they should try to, when we could attend meetings in person, listen to webinars and always mention NIST and NICE and I always mention the IAPP. I always mention a few different forensic companies as well and to learn what's going on, stay up to date, and if you find an issue you're extremely passionate about do further digging and talk to more people about it and maybe write about it. Offer your opinion on what could happen with this tech, what could happen in the field moving forward. I think that the important thing is to really fan the flames of the passion in the field because it's also something so vital for workforce in cybersecurity. They have to be passionate about what they're doing in order to want to stay up to date, stay educated and trained on it, to really accept the intertwining nature between the cybersecurity element of their company but also the actual business of their company, you have to be passionate about it. If I give advice, it's really find the thing you're most excited about within the field and to push forward in it because you have something valuable to say about it let it be heard.

Karen: That's great advice for not only new people in the field but all of us so thank you so much. Thank you for your time today. This was really wonderful. I'm sure our listeners are going to be thrilled to hear your perspectives and we'll look forward to your book next year. Thank you so much for your time today Leeza.

Leeza: Thank you Karen.