Framework in Focus: Eoghan Casey
NICE Newsletter - Fall 2021

Interview Transcript

Karen Wetzel: Hello, my name is Karen Wetzel. I am manager of the NICE Framework at the National Initiative for Cybersecurity Education at NIST. 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 eNewsletter series, *Framework in Focus*, it is my pleasure to speak with Eoghan Casey. Eoghan, thank you so much for letting us learn more about your career pathway and understand the NICE Framework from your perspective.

Eoghan Casey: Thank you, Karen, for the opportunity.

Karen: Eoghan, could you start by explaining with us the work you do in digital forensics and incident response via your consultancy and your non-profit work?

Eoghan: I've come from a long experience in digital forensic work in both the criminal context and the cybersecurity context. My role has evolved to the point where I deal with very complex incidents, and it's a matter of coordinating a number of specialists in different areas to determine the root causes, the extent of the damage, and follow-up actions that might be necessary—whether it's to improve the cybersecurity weaknesses that were exploited or to pursue legal action involving law enforcement, for example.

It's often not fully appreciated that digital forensics plays such a central role throughout the cybersecurity lifecycle to enable the detection of cyberattacks, further scope assessment, assessment of damage across an organization, the development of threat intelligence, and then being able to bring someone to justice as well. It's very central and sometimes undervalued in the process.

Karen: It sounds like fascinating work! Right now in the NICE Framework, forensics and incident handling are separated into different categories, where Protect & Defend includes incident response, and Investigate includes digital forensics. We've heard suggestions in the past that maybe these should be more closely aligned and to also differentiate the law enforcement role in cybercrime investigations. What are your thoughts on that?

Eoghan: There is alignment but also value in separating out some of the skills in incident response versus digital forensic analysis. Another piece of the puzzle is cyber threat analysis. I think it is important to better define and understand the interplay between these different specializations. For example, a single person may fulfill multiple roles, but there is also value in having people who are specialized in specific areas and having those separated out in the NICE Framework is useful. Maybe having some articulation of their relationship can be helpful.

Karen: That's great feedback. We oftentimes need to clarify that Work Roles in the NICE Framework are not equal to job positions or titles. Having clarifications about the relationships could be helpful in understanding how someone might do one independently or, as you point out, may have multiple roles.

Eoghan: Exactly. It's useful for the NICE Framework to now be focusing on Competencies. That can give someone who's looking for employment or an employer looking for someone to employ some gradations and some articulation of what Competencies they're looking for.

Karen: Since the introduction of Competencies in the November 2020 revised NICE Framework publication, we've been doing a lot to build those out so that they can be finalized later this year.

Since we've been talking about work roles, I wonder if you could share a bit more about the people you work with and the kinds of roles that they fill?

Eoghan: When I'm involved it's often in more complex incidents. I work with all phases of the cybersecurity work chain, from the system administrator or security analyst—who is on the front line of defense and who may initially have dealt with problem detection or some of the initial response— through to front-level incident responders. I'll work with them to help get better visibility of the incident, learn what they've gathered and gleaned from their response activities, and provide guidance on what to do and what not to do in terms of evidence preservation and making decisions, which is often at the executive level. This might include deciding to leave the intrusion ongoing while gathering more information—a difficult decision for any organization to accept the risk of leaving malicious actors on their network to observe what they're doing for a period of time—through to more in-depth forensic analysis, where highly specialized individuals look at malware or network traffic to extract additional information and perhaps decrypt information. Those specializations are where we get into a gray area of who is an incident responder and who is a forensic analyst because it is often somebody taking their forensic analysis knowledge and applying it to the incident response process, but at a much more technical level. And then at a higher level, there is the need to translate all this technical detail into the big picture—describing the exposures and options for response, including technical and potential regulatory or legal responses—for decision makers in an organization. Ultimately, if an incident goes into the legal action phase or into law enforcement, there is a testifying role. Usually where I'm involved is at this point of coordination level and then also at the presentation and decision-making level or in court.

I also teach and research to try and bring new members of the community or of a team to a higher level of capability or to develop new methods or tools to help us analyze our information. The teaching and research is critical in terms of keeping pace with the changes in the field.

Karen: Let's turn to that. You are well known in this field and bring a lot of expertise and experience to bear in your work. My question is: How did you get to where you are now?

Eoghan: I started as an information security officer at Yale University, at a time when cybersecurity was, I'd say, in the very early phases. I had a lot of work to do in implementing security mechanisms, intrusion detections systems, firewalls, and the like. But I also had a lot of work to do in responding to security breaches and misuse of the network. I was dealing with, on average, over 300 incidents a year, essentially one a day. So I got a lot of experience with quite a wide variety of misuse of computer systems, not all of it external. As you can imagine, a university is a microcosm of the world. There were all sorts of issues, including cyber stalking and missing persons. In some cases, I had to be involved in criminal investigations that arose out of the community.

Once I had that experience, I worked for a time with EDUCAUSE to bring together other members of the higher education information security community to develop more consistent approaches to dealing with these types of problems. Then I moved to the private sector for a time to get broader experience. I was working as a director of a commercial forensic laboratory, Stroz Friedberg, which is now part of a much larger organization. At the time it was what would be called a boutique kind of consultancy, dealing with very high-profile or complex matters dealing with not just cybersecurity matters but civil matters as well.

That gave me quite a significant amount of expertise with which I was able to go into business for myself. But I found I wanted to help deal with some of the more international problems that were emerging back around 2005. So I started working for the Department of Defense in the DoD Cyber Crimes Center to bring my digital forensic and incident response expertise to bear on state-sponsored attacks against industry and government. That was also a good, broadening experience, both technically and just in terms of understanding the international scope of a lot of these activities.

Ultimately, I decided to focus more on research and development to develop new capabilities in the field. I went most recently for a time into research and development, including as a professor at the University of Lausanne in Switzerland. Now I'm more at the policy level and research level.

Karen: You mentioned competencies earlier. We introduced them in our November 2020 revision of the NICE Framework, and one of the reasons we did so was because of a growing need for a broader and more diverse pipeline. Degree-based education isn't always the best match for emerging technologies, approaches, and policies. What are your thoughts on the role of academic degrees and cybersecurity certifications and how they relate to the practical experience that you are describing?

Eoghan: There is more than one answer, depending on the career path that someone wants to take and on what opportunities are available for that particular person. It's very important to have options for a diverse set of individuals to enter the cybersecurity workforce. We need more people with these skill sets—there's a huge lack of qualified candidates at the moment,

so the broader the pool of people coming into the field, the better we'll be able to deal with these problems.

It's really important to have multiple career and education pathways for high school students coming through community colleges, higher education, or even sometimes directly to the workforce. The NICE Framework, in that context, really helps people entering this career to focus their attention on the areas they need to develop for a job instead of trying to cover everything that is structured in the NICE Framework. So instead they can say, "Okay, I'll focus in this one area to start with and understand what is necessary for that area." It's a step along the pathway to a career in cybersecurity.

When we're talking about people with more opportunities—whether they are going into a college-level degree, already have some existing work experience, or are transitioning from one technical (or even non-technical) career into cybersecurity—having the same view of what capabilities are necessary can help with that transition significantly. It can also help us structure education around the Competencies we need people to be developing as they enter the workforce. Certifications can be very beneficial for people who are trying to get started. Degrees are useful for some of what I view as higher level or more specialized skills sets for some of the work we do.

It's very important to give a map because it's such a broad field. Cybersecurity is in the private sector, public sector, and also research and development. It also includes many different specializations. It can be overwhelming for somebody to enter this field. Having the NICE Framework and steps that people can take to get into a career in cybersecurity is really valuable.

Karen: That's what we aim to do, and are working to build out more supports, as well, such as identifying alternative ways to identify achievements—whether it's on-the-job experience or more formal credentials and degrees—and working with education and training providers to tie content to NICE Framework Work Roles and Competencies.

Moving on to my next question: As you've said, there are a lot of different kinds of cybersecurity work out there. From your perspective, what roles do you think are the most difficult to fill? It might be, for example, an emerging area of need or a high-demand area.

Eoghan: The areas that are easy to fill but just starting are the more technical positions. There is a large need, so that's not to diminish their importance in terms of getting people who have basic competencies in incident response to deal with the growing number of cyberattacks or basic digital forensic analysis skills to do an initial examination of collected data or to even just preserve the data for subsequent analysis.

The most difficult position to fill is somebody who has a combination of the digital forensic expertise—so there's a technical aspect there—as well as programming skills and strong problem-solving or critical thinking abilities. This combination of competencies and skills that

include reasoning is highly valued and is also what makes these jobs hard to fill, so they are some of the highest paid jobs in the field. It takes time and resources to find those people and bring them onto a team. But it also takes time for an individual to get to that level—the combination of education and experience is critical in this field.

Karen: It goes back to the concept of career path too. It's understanding where someone might be now and being able to continually evolve and build those capabilities to get to these kinds of positions. I can imagine that's both on the individual level as well as in the organization wanting to build those capabilities out.

Eoghan: That's a key point. With my career pathway, I consciously looked for opportunities to get different practical experience and also continuously sought opportunities to educate myself. There are some organizations that understand that value and will pay for education and training to help individuals advance, but what happens more frequently is people move from one organization to the next and in the process get broader experience and training.

Karen: My follow-up question, then, is: How have you kept your skills sharp and current? You shared about how you've done a bit of this on your own via identifying where you want to go and what you need to learn, but can you share more?

Eoghan: One of the great benefits of the cybersecurity field is that there's huge willingness to share in the community. Attending community conferences or participating in competitions where there's an opportunity to interact with other knowledgeable members and develop or see new skills sets is what I've done for all of my career. The organization I have been involved with most consistently is the DFRWS, which is focused on digital forensics. Each year it organizes an international forensic challenge. The competition is on the technical side, but in each community event there are small, fun competitions that we call Forensics Rodeos. Those events and the exchange of knowledge, either in person or online, have been my biggest source of keeping up my skills.

Another way I do so is through the teaching and research that I do. It doesn't have to be a full-time job. It's sometimes nice to engage in a discrete training event and share your knowledge with others who are trying to advance in the field, whether in a high school or university or conference context. To teach something you must understand it well enough to explain it, so it's a good learning process and also helps with career advancement.

For research, it doesn't have to be high-level, academic research. A lot of practitioners do very focused and practical research with new technology or a certain type of data, studying it, pulling it apart, and publishing a blog. Sharing that kind of research with the community helps you gain knowledge, learn a new skill, and get feedback from the community.

Karen: This theme of reaching out to and engaging in the cybersecurity community has come up in previous conversations I've had. Certainly, at NICE we have a number of communities of

interest ourselves, including a new NICE Framework Users Group that launched in January this year.

For my next question: I know you're doing some work now that is helping to make our workforce more diverse. I wonder if you could share a little bit more about those efforts.

Eoghan: For the past four or five years, I've been working on a project that was initially funded by the National Science Foundation to educate high school students about cybersecurity and digital forensics. We have a non-profit umbrella organization now called Cyber Sleuth Science Lab where we create curriculum for mostly out-of-school programs, and we've started to do in-school activities and a hybrid of in-classroom and online. It's specifically targeted to traditionally under-represented populations, particularly young women. We've benefited from involvement from partner schools in Baltimore, New Orleans, and Nevada that serve specifically Hispanic communities or African American communities and provide career pathways for those students to enter the field in some fashion.

Throughout my career I've also worked with universities trying to bring more diversity into the cybersecurity and digital forensic fields. I came from a computer science background but had a lot of interaction with forensic science. Computer science does not have a lot of diversity in the workforce. Forensic science, on the other hand, does. Putting the two together has been very fulfilling. I've had the pleasure of being able to bring more individuals from diverse backgrounds into the digital forensic and cybersecurity domain because of their interest in forensic science. Providing education pathways for individuals who wouldn't otherwise have those opportunities is really essential at the high school and higher education levels.

Karen: It's just so very important and not only, as you pointed out, because there's a real pipeline issue here. There's a need for the broader experience and perspectives that a more diverse workforce can bring to the work, to prepare us more effectively while making sure we are adequately staffed in areas of need. Just a couple of last questions. What do you enjoy most about the work you do?

Eoghan: I would say the most fulfilling part of my work is helping people. Whenever someone calls me it's bad news for them, so to help them deal with the problem is fulfilling. I also really enjoy the variety or work—every engagement has unique challenges to solve. I like the challenge, and the diversity of experiences is really fulfilling.

Karen: It's certainly an area that keeps you on your toes.

Eoghan: And provides job security! Unfortunately, we have to get better—instead of paying off the criminals we need to discourage them.

Karen: Getting ahead of it, yes. My last question is: What advice would you give to a young person considering a career in cybersecurity?

Eoghan: It goes back to the combination of education and practice. What is key is to seek work opportunities, including internships. Throughout your career try out different roles in different organizations to see if you actually like them or not. As you do this, you develop your skill sets and it becomes easier for you to take on new opportunities and new challenges.

In the end, it's about finding the right context or the right area to focus on. That's what I've done in my career and what I encourage all the students I teach. I really try and find ways to combine work experience or internships with their education. But we need to have focus and consistency in the cybersecurity education in high schools and universities. Although the NICE Framework provides a structure we can target and adapt or develop, we are looking at multiple frameworks at the moment. At the high school level, for instance, there are standards and frameworks for teaching science, technology, engineering, and math. There are benefits to knowing what we need to teach and for us to evaluate what new members of the community know, what competencies they have, to create kind of a pipeline or a pathway for us to fulfill the growing need for people in the cybersecurity workforce.

Karen: You've given some great advice. Going back to what you mentioned about the importance of engaging in the community I think it's good to remind folks that, as they do move forward, the community is there to help support you and is where you can provide support to others. Eoghan, your work is fascinating and I really appreciate that you took the time out of a busy schedule to speak with us and to share about your experience in this field. Thank you so much.

Eoghan: Thank you, Karen. It was an honor, and I appreciate the opportunity to encourage others or perhaps provide an example of what might work and encourage any future questions as we learn and as we develop the domain. I look forward to using and contributing to the NICE Workforce Framework for Cybersecurity.