"I was always interested in decision-making and what we were finding with when we were studying network defenders is there's an awful lot that they're thinking about in terms of trying to figure out whether they're under attack or how to respond to one. We sat side by side with cyber defenders and we asked them to vocalize what was going through their minds and we started putting together an entire process of what each of the decisions are that a cyber defender makes in the course of determining whether a network is under attack and all the information sources that they need to make those decisions."

MARCH 9, 2020

Psychology in Cyber

Presenter: Anita D'Amico

Summary

Human perception and how we process thought can make all the difference in understanding and predicting attacks. Cybersecurity expert Anita D'Amico, founder and CEO of CodeDX, uses her background in clinical psychology to lead a career conducting research studying decision-making, how human factors affect vulnerabilities, and how perception determines a specific response to an attack.

Transcript

Brian Contos:

Welcome to the Cybersecurity Effectiveness Podcast, sponsored by Verodin. The Verodin Security Instrumentation Platform is the only business platform for security that helps you manage, measure, improve and communicate security effectiveness. I'm your host, Brian Contos, and we've got a really special guest today. Joining me is Anita D'Amico. Welcome to the podcast, Anita.

Anita D'Amico:

Thank you very much, Brian. I'm glad to be here.

Brian Contos:

Anita, you have an incredible background. Before we get into some questions that I have for you, I'd love it if you could share with our audience a little about you and sort of how you came up in the space.

Anita D'Amico:

Well, thanks. I'd be happy to do that. I have a rather unusual background for somebody in cybersecurity. I'm actually an experimental psychologist. I have a PhD in Psychology and I came to cybersecurity in a rather circuitous path. I started out doing research in the Merchant Marine. I was studying why it is that people get involved in accidents at sea. I then moved on to working on the manned space program where I worked on designing the habitation module for the space station and for some displays and controls. I worked on surveillance aircraft, the very beginnings of digital cartography and through an odd series of circumstances, I wound up heading up the first group of information warfare experts at Northrop Grumman.

Brian Contos:

Wow. I don't know what you mean, Anita. It doesn't everybody follow that exact path in cybersecurity.

Anita D'Amico:

Even the way I wound up running information warfare at Northrop Grumman was rather strange. I was at Grumman when Northrop bought Grumman and they selected seven people from Grumman to get inculcated in their culture. We participated in a program management course for two weeks at Northrup. Dr. James Roche, who was an executive vice president at Northrop Grumman, came to speak to our group and he said, the future of this company is information warfare. Do you know what information warfare is? We all sat there not knowing what it was and feeling really stupid. He said, well trust me, that's where the direction of this company is heading. I brazenly wrote a memo to Dr. Roche, who by the way, later on became the Secretary of the Air Force. I said, I don't know what information warfare is, but I can guess what it is. If I'm even partially right, here's 10 things we might do as a company. The next thing I knew, I was running the first information warfare team at Northrop Grumman.

Brian Contos:

Wow. Be careful what you put in a memo.

Anita D'Amico:

Right?

Brian Contos:

No, that's amazing. For our listeners as well, maybe you could give a little background exactly what experimental psychology actually means. If there's some set definition or explanation, because I know for me that was a new term when we first started talking. What exactly does that mean?

Anita D'Amico:

Sure. Well, most people, when they think about psychology, they think about clinical psychology that is going to see a psychotherapist having somebody help you with problems that are mental or emotional. There is an entire other branch of psychology, which is psychological research. There we study human behavior and we try to come up with predictions of human behavior as well as understanding the motivations behind human behavior and how to change human behavior. That's all part of experimental psychology.

Brian Contos:

Very interesting. Okay. Now I'm seeing where some of the dots are connecting here. Let's talk a little about your education [and] psychology, but specifically how that has helped in regards to your work in cybersecurity research and business as well.

Anita D'Amico:

Sure. Experimental psychologists are fairly comfortable with variable behavior. That is ambiguity. Unlike other sciences, human beings tend to be variable on purpose. They don't follow the rules that are followed in biology or chemistry. People will act differently just for the sake of acting differently. If you're trying to study human behavior and find rules and predictions about it, it's rather difficult. The first thing that I think has helped me is that I'm comfortable with variability and not understanding everything, being able to work productively in an ambiguous environment. I think the second thing that has helped me is my understanding of experimental methods. When you're an experimental psychologist, you study both individual behavior as well as group behavior. I have applied that in my research and in business in that I can look at things that are very individual level and the nuances of human behavior within an individual as well as be able to understand patterns of behavior across a group.

Anita D'Amico:

I think the third thing is communication. It's very difficult to communicate to people what psychological principles are. I think that my background has given me a particular skill and being able to communicate verbally and in written form in a very clear way. Notice what I didn't say is that it gave me insight into people. Almost everybody that meets me says, "Oh, you're a psychologist. You must be studying me," or "You must have great insight into people as a result of your education." I actually don't think that's true. I have to be very good at reading a room and I'm also very good at interpreting body language and I think that's been very helpful to me in my business. I don't think that has anything to do with my background in psychology. I just think that's part of my nature.

Brian Contos:

Part of your nature, now that's really... Anita, are there a lot of people from the experimental psychology field that are in cyber that you know of? Is this common or are you sort of that, that rare gem? Because, I don't think I've run into anybody else with a similar background before.

Anita D'Amico:

There are very few of us, there really are. Even when you try to publish research in this area, there are very few pieces of scientific literature to pull on that relates psychology to cybersecurity. There aren't very many of us. I have found my psychological background to be very helpful in doing cybersecurity research.

Brian Contos:

Yeah. I would guess, and this is completely a guess, but I would guess that most of the research that's being done, or most of the papers that are being written as it relates to cybersecurity and psychology are probably predicated a lot on social engineering and things of that nature. Juxtaposed to many of the facets that you've mentioned, which I find are fascinating.

Anita D'Amico:

That's absolutely true. I think the two big areas that psychology is having an impact on is the social media and this understanding cybersecurity and social media. The other is privacy. There's an entire body of research on how people perceive privacy and that's a form of cybersecurity.

Brian Contos:

Yeah, that's an interesting one. I think that'd interesting one to see how it's trended out over the last few decades and predictions on where it's going just because I think some of these generations coming up are living in a world where maybe privacy isn't seen the same way or thought to even exist maybe in some cases. That would be some

interesting research to read through. Anita, you've been exposed to so many different areas. Your work in the private sector, your work in the public sector. Are there specific areas where you have directly applied your experience in psychology to gain insights to what we classically think of as a cybersecurity problem?

Anita D'Amico:

There are a couple of areas that I have worked on in my career that relates specifically to the psychological principles to cyber security. I think one of the first area that I got involved in was actually visualization of cyber events. I started studying people who were trying to find attacks in a network and they were inundated with all of these alerts and we experimented with different ways of visualizing those alerts so that they could visually correlate different events to each other and see patterns in an attack. Now that type of work in visualization of cybersecurity pulls on one's understanding of human perception. For example, the way people perceive color and shape affects the way they process the information. It also pulls on an understanding of how people relate objects and concepts to each other and in decision making. The first area that I got involved in cybersecurity in a big way was in visualization.

Anita D'Amico:

I've also studied decision-making. I was always interested in decision-making and what we were finding with when we were studying network defenders is there's an awful lot that they're thinking about and in terms of trying to figure out whether they're under attack or how to respond to an attack. I did research where we sat side by side with cyber defenders and we asked them to vocalize what was going through their minds and then we wrote those things down and we started putting together an entire process of what are each of the decisions that a cyber defender makes in the course of determining whether a network is under attack and what are all the information sources that they need to make those decisions. Where are the gaps in their knowledge or even where the technology is hindering their decision making.

Anita D'Amico:

I did that type of work for a while. In fact there's a term for that and it's called cognitive analysis. Then I think the last area that I've been working in more recently is human factors that affect secure code development. Brian, did you know that most cyber attacks can actually be traced back to an attacker exploiting a software vulnerability?

Brian Contos:

Sure, sure.

Anita D'Amico:

That vulnerability gets in there by a programmer who accidentally put it in there, introduced the vulnerability, and I got very interested in the topic of why is it that some developers are more likely to develop vulnerable code than others or which teams are going to develop a more vulnerable code than others. I'm currently engaged in a research project that is studying the human factors. For example, a developer who doesn't get a good night's sleep, they more likely to write insecure code? What about the size of a team? If you have two people working on a code base, is that likely to be more or less secure than if you have eight people working on a code base? We're also looking at factors related to the number of interruptions. When you talk to a developer, they often talk about being in the flow, I need to be in the flow. It's really to engage in deep work. Well if you interrupt that flow, is it likely to result in less secure code? That's my most recent area of research.

Brian Contos:

Wow, that's fascinating. It really is. It's nice to know that somebody is researching at that level and that type of detail in this arena just because I think it makes a ton of sense, especially as it relates to incident response visualization. It's funny when you start talking about that. I was thinking about my days at ArcSight and when we are doing visualization for SIEM, so we had all this log data coming in from all these network and endpoint sources and operating systems and everything else and we go, boy, I bet there's some cool things we could do. There really were, what we found was the way a DDoS attack is visualized is different than lateral movement, is different from beaconing or a malware execution. And they actually create pretty interesting visuals so much so we actually had them turned into artwork and then eventually stickers that we give out at the local conferences.

Brian Contos:

Because people really dig the way that these things look from a visual perspective, being able to visualize what a DDoS attack might look like. I remember in that process the amount of time and effort when you're talking about visualization, to your point that goes into the size, the shape, the color, the layout. I can't remember how much time

we spent, which way should the shadow fall on the actual representation to look at it. That type of research I think is fascinating because when you're doing analysis as you well know, it's far easier to see a visual that represents what's going on than trying to pour through gigabytes and gigabytes a day to make a determination. It might take you days or weeks, and that way we're looking at a visual could happen in a matter of seconds or minutes. That's really interesting.

Anita D'Amico:

Oh yeah. People are really good pattern detectors and they're particularly good at detecting visual patterns. In applying visualizations to cybersecurity, we used the power of human detection of patterns to facilitate the use of visualizations. There are a lot of psychological principles that effect a good visualization. The way people perceive color, the way they group things together in their mind, even though they may not look like they group together visually, there certain rules that guide a human perception. I used to have a little road show that I did where I would say, here are the rules of human perception and now let's take a look at some visualizations. I would pull up product visualizations and either say this is a good visualization because of these things or sort of have the Rogue's gallery of bad visualization.

Brian Contos:

Yeah, I bet that was fascinating. I've seen some interesting ones over the years. Sometimes you see them, you're like, wow, this is really cool. There's like three-dimensional spinning globes and laser beams and this and that. You're looking at it, you go, I have no idea what it means. It's cool to look at, but I don't know what it does.

Anita D'Amico:

There's a difference between cool and informative.

Brian Contos:

That's right. Anita, I know you're focusing a lot today on application security and you're doing a lot of work in that area and you mentioned a few caveats of that before, but what are maybe some big ticket items that you're working on at applications security today?

Anita D'Amico:

I'm heavily involved in application security. Code DX is the company I run and we are an automated application security management system. The issues that I'm trying to address in our business is that application security is a disjointed, time consuming, and painful process. As I noted before, most cyber attacks start with an attacker exploiting a software vulnerability. You really need to get rid of those vulnerabilities before you go into production of the code. Discovering the security weaknesses and remediating them is very time consuming, disjointed and painful. What I've been working on and our staff at Code DX, are ways of automating that process, improving the workflow. We're working on the ability to make it a lot more efficient to do application security from testing of the software to the discovery of the security weaknesses. We help prioritize the weaknesses so you know which ones to fix first. Then we track the entire remediation process. That's what I'm working on right now.

Brian Contos:

Very cool. Very cool. Anita, as we wrap up here, there's a question I like to ask everybody on our show and that's who is your favorite superhero or supervillain and why?

Anita D'Amico:

That's an easy one for me. Batman. Batman is my favorite superhero because he does not have super powers. He fights crime using his intellect, his personal motivation, innovative technology and, of course, his abundant wealth. He's a person who suffered a tragic loss and turned his grief into the energy to fight crime. I feel as though Batman is somebody that many of us can try to become, if we use our passion, our intellect and innovation to achieve our goals.

Brian Contos:

I love it. I love it. Always be yourself, unless you can be Batman, in which case, always be Batman.

Anita D'Amico:

My favorite supervillain is the Riddler because first of all, I love puzzles and riddles. I like the way the Riddler uses puzzles and riddles in the perpetration of his crimes. It's part of his strategy. Again, it's an appeal to the intellect. Of course, I love the way Jim Carrey played him back in the 1990s.

Brian Contos:

Yeah. It's always nice when you can wear a suit with a bunch of question marks on it as well, for your evildoer outfit. Now that's awesome. Thanks so much, Anita, and thanks to our listeners for joining and be sure to check out other Cybersecurity Effectiveness Podcasts, sponsored by Verodin.