The Cybersecurity Readiness Podcast Series

Episode Title	Proactive Resilient Approach to Cybersecurity
Podcast Series	The Cybersecurity Readiness Podcast Series https://www.dchatte.com/podcast/ https://the-cybersecurity-readi.captivate.fm/
Host and Producer	Dave Chatterjee, Ph.D. https://dchatte.com
Guest	Kriti Arora, Security Global Black Belt, Threat Intelligence and Enterprise Attack Surface Management, Microsoft
Summary Pitch	It is well known that a proactive intelligence-driven approach to cyber governance is the way to go. But it is easier said than done. Embracing and sustaining such an approach requires an extremely high level of commitment, preparedness, and discipline. Kriti Arora, Security Global Black Belt, Threat Intelligence and Enterprise Attack Surface Management, Microsoft, shares her experiences of guiding clients to adopt an intelligence-driven proactive approach to thwarting attacks. She also shares her passion for the field and the satisfaction of training and serving as a cyberwarrior.
Time Stamps	00:48 -- Before we get into the details of a proactive resilient approach to cybersecurity, how about sharing your professional journey? What got you into this field? 03:58 -- You described yourself as a first-generation cyberwarrior during our planning meeting. I found that quite intriguing. Please expand. 06:54 -- Can you shed some light on the different types of opportunities that a cybersecurity career can present to the first generation (of cyber warriors) or people trying to pivot from their existing careers into cybersecurity?

	11:14 -- Kriti, share with us briefly about your role at Microsoft? At a generic level, could you share what you do at Microsoft with the listeners? 15:16 -- What is a proactive, resilient approach? 18:08 -- Why do organizations vary in their level of proactiveness? What are some reasons? 21:10 -- What are the five or six things one should do to get started on the path of proactiveness? 27:43 -- Maintaining a log of security intelligence received, and actions taken might be very useful, especially when an organization is trying to defend itself in a court of law. What are your thoughts? 34:24 -- Every organizational member has a role to play in securing the organization. Do you agree? 36:28 -- Asset prioritization and data retention strategies are key aspects of proactive cybersecurity governance. What are your thoughts? 40:59 -- What measures or metrics are useful in assessing proactive resilience? 45:02 -- Please share some final thoughts and key messages for our listeners.
Memorable Kriti Arora Quotes/Statements	"So, at one moment, you're fighting crimes, doing these investigations like a detective, and researching a problem to find a solution. At another time, you could be troubleshooting a typical problem and providing customer support services." "The adaptive quality of the field is what makes it thrilling. That's what excites us, the cyber warriors, who are trying to experiment, learn new things, and save the world with different techniques and tactics." "I consider a proactive approach to be intelligence-driven and holistic. It represents a mind shift on how cyber threats are thwarted."

	"In this proactive approach, we focus on indicators of attackers; we try to keep a watch on the entire network and its processes. It's a holistic approach. I would not call it a technique; I would call it a mind shift because you need that mind shift to understand proactiveness. It's like being alert, thinking about the worst-case scenario, trying to prevent it or be prepared to recover from it quickly." "It's very important to focus on the attack surfaces, whether internal or external. A full or 360 view of your attack surface is very important." "Successful implementation and sustenance of a proactive resilient approach depend on a high level of cybersecurity awareness and knowledge." "Organizations must strive to be both secure and productive."