The Cybersecurity Readiness Podcast Series

Episode Title	Ignorance is not bliss: A Whole-of-Enterprise Approach to Threat Management
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	Anne Leslie, Threat Management Consultant, IBM Security
Summary Pitch	The incredibly articulate Anne Leslie, Threat Management Consultant, IBM Security, shares some powerful messages and recommendations on threat management. One such message is to nurture a Whole-of-Enterprise approach where "leaders believe that the people who work for them are not just as important as the systems and the data, they're more important." Anne also emphasizes the importance of "looking within and knowing what it is that we have, why people might want that, and how they might go about getting it."
Time Stamps	00:42 -- So, let's begin by talking about the major information security threats out there and you being in Europe, we'd love to get that perspective. 05:49 -- Anything that you see out there by way of best practices, in terms of staying on top of the latest attack vectors and methods. 10:43 -- I'd love to hear your perspective on a human-centered cyber defense strategy. 19:20 -- I read in the media reports that organizations are often slow, and for lack of a better word, negligent in promptly and effectively responding to

	cyber intelligence. This is definitely a weakness that no organization can afford. What are your thoughts? 29:38 -- I'd love to get your thoughts on joint ownership and accountability, or shared ownership and accountability? 38:44 -- Any final thoughts?
Memorable Anne Leslie Quotes/Statements	"So one of the things that I notice in our industry, across businesses, is that we have a tendency to look outwards before we look inwards. And in practical terms, what that means is, we're not very clear collectively about what it is in our organizations and our businesses that adversaries might want." "Let's start with looking within and knowing what it is that we have, why people might want that, and how they might go about getting it. If we already have answers to those questions, we're on a good footing." "I believe that people come to work every day with an often unarticulated aspiration to be useful. And it just seems to me that we're totally missing out on capitalizing on people's best intentions and their creativity and their motivation - when we label them weak when we label them as a vulnerability against which we need to defend." "People want to contribute, people want to be helpful, they want to be united in something that's a little bit bigger than themselves. And security practitioners, in particular, maybe not all of them, but the majority that I've interacted with, are driven by a desire to protect, they're driven by a cause. To them, security is more than a job, it's a cause they want to defend."

	"It's not just about buying more technology, It's about doing more with what we have, where we are. And making the most of the capability that we can get from our people is a key factor in that." "I loved what you just said about the impact of security being positively correlated with the health of the culture in the organization. Yes, a million times, yes! Because when you have a healthy organization - which is built up consistently, with consistent behaviors, consistent attitudes, consistent interventions on the part of leadership - what it instills, in people at every level of the organization, is a sense of accountability, a sense of responsibility, a sense of pride. And most importantly, it instills a desire to protect, because people have an emotional connection to their organization and an emotional connection to the leadership, even if they've never spoken to them."