The Cybersecurity Readiness Podcast Series

Episode Title	Bridging the Gap Between Intentions and Practicality in 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	Daniela Almeida Lourenco, Chief Information Security Officer (CISO) at Tinka
Summary Pitch	Daniela Almeida Lourenco, Chief Information Security Officer (CISO) at Tinka, firmly believes that CISOs have the very best of intentions -- "we all mean the best; we all want to protect the organization, and that is all we want to do." However, often the reality of the Board's lack of a cybersecurity mindset coupled with insufficient budget and resources results "in a reactive posture, unpreparedness, unclear risk management strategy, and low response maturity." She also highlights "the misinterpretation and implementation of the lines of defense model" to be another reason why right intentions do not get translated into good practices. Advocating for a more hands-on senior management role, Daniela says, "if you're on the second line of defense, you're not supposed to just sit on your highchair and disconnect from Operation." She also expresses concern about the excessive use of the 'fear factor' in cybersecurity communications. Finally, Daniela recommends against reinventing the current culture but making suitable adaptations by embedding new practices.
Time Stamps	01:15 -- Share with us a bit about your professional journey.

	04:26 -- Share with the listeners why this topic or theme appealed to you. 07:56 -- What's stopping an organization from being proactive? 12:55 -- Based on your experience and your understanding of sociology and psychology, what recommendations do you have to change things up, make them (senior leadership) more optimistic, make them more proactive, make the stance (cybersecurity stance and approach) more optimistic, make the stance more proactive? 18:54 -- Cybersecurity is everyone's business, and everyone has a role to play. It's just like the way we are fighting the pandemic. We cannot just rely on the healthcare professionals to do everything for us, we also have to do our part. And I think that's kind of similar to how we need to deal with the cyber attacks epidemic. What do you think? 21:17 -- Gamification can be perceived in some cultures, such as the German culture, as something not very serious; you're not being serious about it. Is that a fair interpretation? 22:37 -- What are your thoughts on the check-the-box mentality toward cybersecurity governance? 27:09 -- In my book, I talk about creating structures and mechanisms that will enable shared ownership and responsibility of cybersecurity initiatives. What are your thoughts? 30:53 -- What are your thoughts about the significance of prompt threat intelligence processing? 36:13 -- Please share your final thoughts and any additional points that are very relevant to this conversation.
Memorable **Daniela Almeida**	"Most practitioners say that they fell into information security by accident."

Laurenco Quotes/Statements	"There is a major or official priority over information security, but it's usually reactive." "One of the things I do see with my peers in the industry is that we all mean the best; we all want to protect the organization, and that is all we want to do." "Only after major breaches and losses does information security come to the agenda. So it's an afterthought." "We've been building an ivory tower, and this ivory tower increases the gap between them and us, and I kind of tend to blame it on the misinterpretation and implementation of the lines of defense model. So you know, the first line as being Operation, and if you're on the second line, in my view, you're not supposed to just sit on your high chair and just disconnect from Operation." "One of my favorite pain points is the excessive use of the fear factor in cybersecurity communications." "One of the major things we're not doing is not knowing the organization and trying to impose a culture where it just turns out to be a counterculture; in the end, it won't work." "What I would like to make very clear to everybody listening is that you cannot create a culture. And sometimes you hear that even on the news and or in other forums. You cannot create a culture. The culture is already there for 1000s of years, hundreds of years. It's a complex beast of old sets of values and norms. What you can do is embed new practices in it." "Make sure that for awareness, you think of three things, explain the risks as they are towards different audiences in your organization, how they can protect themselves from them, and how to contact you if something seems abnormal." "My advice would be, try not to invent the culture again, learn from the culture of the organization, try to adapt to it from within, and manage

	the expectations that the stakeholders have and listen to organization in all of the sectors, spend time with the core operations, spend time with everyone in your organization to understand where the risks are, where the opportunities are, and listen to the needs, because that's the foundation of everything that you've been built from then on."