The Cybersecurity Readiness Podcast Series

Episode Title	Cybersecurity is Patient Safety
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	Stoddard Manikin, Chief Information Security Officer, Children's Healthcare of Atlanta
Summary Pitch	"Cybersecurity is patient safety and patient safety is cybersecurity," is how Stoddard Manikin, Chief Information Security Officer, Children's Healthcare of Atlanta, described the significance of cybersecurity readiness in the healthcare sector. Speaking with exceptional clarity and eloquence, Stoddard traced the evolution of the cybersecurity threat landscape and governance approaches, before discussing in detail what it takes to succeed as a modern CISO.
Time Stamps	01:35 How would you describe the evolution of the cybersecurity phenomenon and what has stayed with you by way of lessons learned? 05:17 Talking about specialization, getting the right people for the right kinds of roles in cybersecurity is very critical. And there are challenges there. But at the same time, you also need the non-cyber security professionals, the members of the organization to do their part. Don't you agree? 06:55

	What are your recommendations when it comes to cybersecurity awareness and training? 10:41 What are some metrics or KPIs that are being tracked or should be tracked? 13:37 What does it take to make a CISO, and when I say CISO, I mean the CISO function as a whole, effective? 17:35 From a practical standpoint, how feasible is it to involve legal or to work with legal closely? 19:59 How and to what extent does your function partner with Legal when formulating and reviewing cybersecurity strategies? 22:25 How do you stay on top of industry regulations and compliance requirements? 24:18 What is the state of cybersecurity readiness in the US healthcare industry? 28:40 Is it common practice to regularly test the disaster recovery capabilities of an organization? 30:46 What are your thoughts on the practicality of conducting real-time security audits?

	33:19 According to media reports, many of the breaches that have happened, large breaches, major breaches, the story goes that the organization was made aware, or a particular individual was made aware, who did nothing about it. Based on your experience in the field, how or why does that happen? 36:03 How feasible is it to have structures and mechanisms to ensure joint ownership and accountability both within the organization, as well as when you're partnering up with vendors? 40:23 Any final thoughts for the audience?
Memorable Stoddard Mannikin Quotes/Statements	"Cybersecurity is everyone's responsibility within an organization. We're past the days where you have a few people in a room providing all the security to the organization, and it's just up to them to take care of it. It's now a central team coordinating cybersecurity for an organization but directing a lot of different players." "And when it comes down to it, people are the easiest way to breach an organization's security defenses. So it's incumbent on every organization to train all of their users that have access to IT resources, and equip them with the knowledge and awareness they need, so that they can be prepared, should someone target them with some kind of attack or attempted attack." "I find that providing them specialized training, giving them a forum to ask questions, testing them on it, perhaps even monthly with a simulation exercise is how you get the best behavioral response. The other part of that training is it can't just be one way where you're giving them the info; the next step is to test them on it. And then the step after that is to measure them on it."

	"First and foremost, the most fundamental thing you've got to know as the CISO is the business of the organization that you're in. Because if you don't understand how the business operates, what it does, how it earns money, how it spends money, where it really makes its profit that funds other areas that have losses, then it's very hard for you to understand how to prioritize what security controls need to be put in place, and also how restrictive you can be without cutting off the lifeblood of the organization." "So a patient can recover from a data breach, but they might not be able to fully recover from lack of care. So that's where I really want to emphasize that cybersecurity is patient safety. And we all have to take it seriously, regardless of where we are in that healthcare ecosystem."