The Cybersecurity Readiness Podcast Series

Episode Title	What Does Good Cyber Governance Look Like? A Legal Perspective
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	Rois Ni Thuama, Ph.D. (Doctor of Law), Head of Cyber Governance, Red Sift
Summary Pitch	From the standpoint of cybersecurity governance, how does an organization stay on the right side of the law? Rois Ni Thuama, Ph.D. (Doctor of Law), Head of Cyber Governance, Red Sift, spoke with great clarity and eloquence in explaining what it means to practice good and sensible cyber governance. She emphasized the importance of looking to expert sources and established security frameworks for guidance, addressing foreseeable and avoidable threats, and making cybersecurity investments that would be deemed (by the courts) proportionate and affordable. Highlighting the importance of strong governance, Rois said, "it is never the widget that's the problem, it is always weak leadership, weak governance, lack of accountability, lack of responsibility, these are the big issues that need to be addressed." She also encouraged a regular legal review of cybersecurity practices, based on the assumption that "you have to defend your decision-making in a court of law."
Time Stamps	1:55 -- What does it mean to practice good and sensible cyber governance? 5:21 – From a legal perspective, what are the key elements of a robust cybersecurity program? 7:02 – What should be some lessons learned from cybersecurity breaches that organizations have experienced?

	12:37 – Is there any best practice that you see out there in terms of how best to incorporate legal or embed legal in cyber governance? 20:14 – How effective are the current laws and regulations to demand top management commitment towards strong due diligence? 26:16 – Organizations could benefit from simulated exercises to assess their legal vulnerabilities in the event of different forms of attacks. Your thoughts? 29:27 – It is important to raise the overall level of awareness of being on the right side of the law when it comes to cybersecurity preparedness. Your thoughts? 32:00 -- What advice do you have for global organizations to be on the right side of cybersecurity laws and organizations of different countries? 36:55 – From a legal standpoint, could one put together a more ironclad agreement whereby the vendors have a little more skin in the game? 41:50 – Any final thoughts?
Memorable Rois Ni Thuama Quotes/Statements	“We are not going to be able to tackle everything, but you don’t need to be able to tackle everything. But you do need to be able to address reasonably identifiable circumstances, that could lead to malfunction, capacity overrun, failure, disruption, impairment, misuse, all of those bad things right." "When you come to court, you really want to nail down everything that is foreseeable and avoidable. Whatever size your firm is, what's reasonably foreseeable and what's avoidable, address those.” "When you look at big corporate scandals or breaches that have a physical effect, it is never the widget that’s the problem, it is always weak leadership, weak governance, lack of accountability, lack of responsibility, these are the big issues that need to be addressed and it is the same with cybersecurity."