The Cybersecurity Readiness Podcast Series

Episode Title	Is Cybersecurity Regulatory Compliance Good Enough?
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	Dixon Wright, Vice President, Vice President, Compliance Management and Automation Platform, Coalfire
Summary Pitch	"The story of the RMS Titanic has served as a grim reminder that regulatory compliance does not guarantee safety or security. The ship was carrying 2,224 passengers and crew when it sank one April night in 1912, killing over 1,500 people. The designers of Titanic had followed the British Board of Trade by equipping it with 20 lifeboats, and even threw in four more than the regulations required." (securicon.com) Dixon Wright, Vice President, Vice President, Compliance Management and Automation Platform, Coalfire, speaks to the importance of moving beyond the check-the-box approach and engaging in substantive information security compliance efforts. He recommends the judicious adoption and use of appropriate compliance management and automation platforms.
Time Stamps	01:55 Yeah, let's talk about your passion. What gets you passionate about information security compliance? 03:15

	For the benefit of the listeners, please provide an overview of information security compliance and the current state of affairs. 06:16 Trying to stay on top of all these different compliance requirements can be an extremely challenging proposition. What do you think? 09:15 How do we ensure that check-the-box behavior is not encouraged? 12:46 I feel this discussion on compliance needs to be coupled with the discussion on governance mechanisms, and measures, which ensure that the tools that are being leveraged effectively and essentially, people are doing the right thing. Your thoughts, your reactions? 16:33 What does it take to create a robust cyber secure cybersecurity compliance program? In other words, if you could highlight some of the key elements of a robust compliance program? 22:24 So going back to automation and compliance, I know your organization has developed a platform to provide those services. When an organization is considering investing in such tools and capabilities, what guidance or recommendations do you have for them? 31:25 What else do you think listeners could benefit from learning about compliance management from an information security standpoint? Or

	anything else that you think is pertinent to this discussion that we haven't talked about yet? 37:05 Let's conclude with a few final words that you may have for our listeners.
Memorable Dixon Wright Quotes/Statements	"We hire really expensive, technical people. And 60 to 70% of their job is being a technical writer." "All these different kinds of industries and sectors have created their own types of standards, and now all these organizations have to comply with them." "There's a challenge of getting compliant, and then there's an even greater challenge of actually maintaining it." "I think, in many cases, compliance is just sales. You're just doing it so that you can sell to other companies, it's not actually used as a mechanism to secure things internally." "We need better assurance that what is being automated is legitimate."