

The Cybersecurity Readiness Podcast Series

Episode Title	Making Cybersecurity Communication Effective
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	Marcin Ganclerz , a subject matter expert
Summary Pitch	Cybersecurity communication should be simple, immersive, attractive, continuous, and multi-channel, says Marcin Ganclerz , a subject matter expert. He passionately argues for creating a 'culture of enablement and not fear' so employees can play a vital role in enhancing cybersecurity communication effectiveness. Marcin also shares several examples and best practices in support of his recommendations.
Time Stamps	00:42 Martin, how about sharing with listeners a bit about your professional and cybersecurity journey? 03:10 How about we start with some challenges and hurdles that are associated with effective cybersecurity communication. 07:18 What would you consider are the key elements or attributes of effective cyber communication? 13:43

	<p>So let's talk about some best practices or guiding principles that you see out there.</p> <p>22:56</p> <p>You said the education about cybersecurity should be permanent. Tell us a little more about that.</p> <p>38:29</p> <p>So I'd like to ask you to start wrapping this up by sharing some key messages, some final thoughts, whatever you'd like to share with the listeners</p>
<p>Memorable Marcin Gancierz Quotes/Statements</p>	<p>"The technical experts suffer from the curse of knowledge."</p> <p>"We should show employees, show users, why cybersecurity is so important for them. And I think the best way to do it is to show them that it applies to their personal life."</p> <p>"Cybersecurity communication should be simple, immersive, attractive, permanent, and multi-channel."</p> <p>"When we treat people as a strong link, they act as a strong link."</p> <p>"Concentrate on building a culture of enablement, rather than a culture of fear."</p> <p>"People love to feel valued. They want to be an important part of the cybersecurity system."</p> <p>"If you have the right culture, people will feel responsible for cybersecurity, they will feel like a vital part of the cybersecurity system and they can be your really valuable asset. But remember, you have to educate them, train them and reward them, not blame them."</p> <p>"Employees can be valuable assets for the organization, but we have to educate them, train them, and reward them."</p>

	<p>"So if you want to build a great culture in your organization, you have to reward your employees, show them that they are important."</p>
--	--