The Cybersecurity Readiness Podcast Series

Episode Title	Is Cybersecurity a Moving Target at Academic Institutions?
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	Tej Patel, Vice President, and CIO at Stevens Institute of Technology
Summary Pitch	In a highly engrossing and in-depth discussion, Tej Patel, Vice President, and CIO at Stevens Institute of Technology, sheds light on the various information security challenges that plague academic institutions and how best to deal with them. He talks about establishing a highly collaborative and security-centric culture, structuring an ideal CIO-CISO relationship, effective execution strategies, and more.
Time Stamps	01:57 Why don't you give listeners an overview of your professional background? 02:57 Let's begin by discussing the information security challenges that academic institutions face. 05:17 So the challenge lies in enabling the university pursue its mission as safely and securely as possible. Is that a fair understanding of the fundamental challenge?

	09:09 How do you keep up with all the activities that are going on across campus or at satellite locations if you'll have satellite locations? What's the mechanism in place whereby you would be forewarned, people will feel the need to say, hey, we need to talk to the security office, because this has some serious security implications, and we want to make sure that we are doing it the right way. 13:44 How feasible is it to offer customized guidance to the various operating units at an academic institution? 16:23 What is your vision of an ideal CIO-CISO relationship? 21:40 If you could share an example of how you and your team brought about a change in the security culture at your institution 25:03 What steps do you all take to secure the student population as best as possible? 30:25 People are busy, they have to deal with so many things. So that becomes another chore where you are expected to diligently look through every email and see whether any particular email deserves to be reported. Where are you on this? What's your perspective? 35:25

	How should organizations prepare for cyber attacks? And what does it take to execute plans effectively in a sustained manner? 39:49 I'd like to give you the final word.
Memorable Tej Patel Quotes/Statements	"Cybersecurity is a moving target in higher education." "Cybersecurity is a shared responsibility to provide a protected cyber infrastructure on campus." "Building trust and relationship are so critical; that allows my team and me to have a conversation with our researchers to fully understand what exactly they are trying to achieve." "There are a lot of things that we have changed in our practices to ensure that we instill the culture of cybersecurity in our business from day one." "It's not so much about reporting structures, it's more about how a CISO and CIO can partner together to deliver the message that cybersecurity or security is a strategic value service for any institution or organization." Nowadays, the role of the CISO and the CIO is more geared toward reducing business risk. It's all about risk management. "Organization must spend sufficient time, effort and resources to build a security-centric culture." "It's not so much about reporting structures. It's more about how a CISO and CIO can partner together to deliver the message that cybersecurity or security is a strategic value service for any institution or organization."

	"The role of CISO and CIO, in my view is more towards reducing the business risk nowadays." "They expect the cybersecurity economy to grow to $10 trillion by 2025." "You have to go back to the basics, do the basics right. Make sure you're transparent, make sure you find good people on your team who are stewards of good security hygiene and do your best efforts daily." "The majority of the breaches happen not through any highly sophisticated cyber attacks. They happen because basic controls are lacking, fundamental training hasn't been provided, unsatisfactory patch management, and more." "We also pay very close attention to finding that balance between user experiences and maintaining the security." "Someone recently shared some statistics about cyber attacks. It happens every 39 seconds. The ransomware attacks are targeted every 14 seconds, and only 10% get reported."