The Cybersecurity Readiness Podcast Series

Episode Title	Protecting Academic Institutions from Ransomware and Other Forms of Cyber Attacks
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	Garry Scobie, Deputy Chief Information Security Officer, The University of Edinburg
Summary Pitch	Educational institutions have been the target and victim of ransomware attacks. Garry Scobie, Deputy Chief Information Security Officer, The University of Edinburg, spoke at length with Dr. Dave Chatterjee on protecting academic institutions from ransomware and other forms of cyber-attacks. The very engaging and informative discussion covered a lot of ground ranging from identifying the most significant threats to reviewing the challenges of dealing with such threats and making recommendations on how best to secure the academic institution and its stakeholders. Garry shared several good practices, one of which was creating the Champions Network to enhance cybersecurity awareness.
Time Stamps	3:20 – What do you see as the single biggest threat right now? 5:51 – How do you go about protecting the organization and its people from ransomware attacks? 7:44 – Students engaging in risky online behavior, the open and interconnected university environment, and budgetary constraints are common challenges when trying to secure academic institutions. What are your thoughts?

	10:04 – Could you speak to the importance of education and training to reduce the risk of cyber-attacks? 12:51 – Is there anything in particular that academic institutions should be doing when it comes to offering cybersecurity training programs? What are some key elements of an effective cyber training program? 15:05 – How do you create an atmosphere where the internal customers feel comfortable coming to you for advice and recommendations and you are able to engage in a candid conversation? 18:16 – How you effectively communicate information security-related information? What incentive mechanisms are likely to further motivate the user community to seek and comply with the information security guidelines? 20:41 – There are some positives to the academic units being responsible for securing their data and related digital assets. Along with the authority, comes the responsibility, comes the accountability. Your thoughts? 22:36 – How would you create information security awareness among students, help students make good decisions? 25:59 – What are the kinds of things you would do at the backend knowing you have vulnerabilities at the frontend? 28:57 – What are some other threat vectors that concern you? 31:21 – What is a good day for you at a professional level? 34:12 – Is no news good news?

	36:15 – Are you likely to gain greater stakeholder attention and cooperation by doing a presentation about the different threat scenarios and their consequences? 40:37 – How do you ensure that intelligence test reports are immediately reviewed and acted upon? 42:04 – What advice and recommendations would you have for peers at other academic institutions? 45:23 – How do you assess cybersecurity performance at an academic institution? 50:32 – Any final thoughts?
Garry Scobie's Memorable Quotes/Statements	"The solution needs to be appropriate, affordable, proportionate, and realistic to the perceived level of threat. It is all about taking balanced risks." "At the end of the day, it is all about the basics and doing them well. The basics are the hardest thing to do and get it right. It is all about people, patches, and processes." "I am paid to be paranoid."