The Cybersecurity Readiness Podcast Series

Episode Title	Countering Insider Threats: The Seven Commandments
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	Dr. Eric Lang, Ph.D., Director, Personnel and Security Research Center (PERSEREC), United States Department of Defense
Summary Pitch	Research finds that there was a 44% increase in insider threat incidents across all types of organizations, and 56% of the reported incidents were due to negligence. Equally alarming is that the average annual cost to remediate a negligence incident was $6.6 million. Dr. Eric Lang, Ph.D., Director, Personnel and Security Research Center (PERSEREC), United States Department of Defense, draws upon his research to share some of the (science-based) commandments for understanding and countering insider threats. Emphasizing the criticality of the human factor, Dr. Lang contends that "without individuals' sincere commitments, the most extensive insider threat policies will fail."
Time Stamps	02:27 -- So Eric, let's first talk about yourself and your professional journey. 04:36 -- What motivated you to write the article Seven Commandments for Understanding and Countering Insider Threats? 07:51 -- The first commandment states that "Human factors are paramount. Thou shalt not worship technology above personal and social dynamics solutions." Tell us more about it.

	15:16 -- Moving along to your second commandment, you say, "Employees are an organization's greatest strength, especially for identifying insider threats. Thou shalt improve supervisory and co-worker reporting." Many employees are reluctant to report potential threats they encounter. I would assume organizations recognize the challenges and have appropriate structures and mechanisms in place to encourage more honest reporting. Your thoughts? 20:45 -- Many psychological factors could come in the way of somebody alerting the organization about a possible insider threat. Thoughts? 26:36 -- I will be very surprised if great organizations, when they make decisions to improve cybersecurity, governance, cybersecurity readiness, those decisions are not influenced by experts in human psychology, the clinical psychologist, or whoever the right person is. Thoughts? 31:07 -- A reactive approach to cybersecurity governance doesn't cut it. Thoughts? 38:37 -- So let me ask you, what do you think are any of the top three things that most employees care about for their job? 43:33 -- Before we conclude, if you'd like to share a few final thoughts.
Eric Lang's Memorable Quotes/Statements	"It turns out that non-malicious insiders were responsible for the majority of the (exfiltration) incidents." "73% of the successful exfiltration incidents were conducted without using technology."

	"Technology is necessary but not sufficient, humans will find a way around it. And in this case, 73% succeeded in the exfiltration." "What was a common successful method for foreign adversaries to get sensitive US industrial information? The answer is they asked for it. It was a form of social engineering in very many cases." "Technology miss performs not because of malicious intent, but because it was ill-developed." "So why do employees in an organization with a See Something Say Something policy, often hesitate to report? There are a number of social psychological factors such as 'don't be a snitch' cultural norm. They don't want a coworker to lose their job. They might have a fear of retaliation." Social psychologists often attribute it to "diffusion of responsibility" when people don't report a potential exfiltration incident. "If you are aware of something of potential concern, and there are many other people also in the environment, you might think that many people have the same awareness I do, I'm sure someone else will report it. This is called "diffusion of responsibility" in social psychological research." "Policy is important, but the execution of it, and bringing employees into correct awareness and engagement is the most important thing." "There can be a disparity between policy and perception because employees act based on their perception, understanding, concerns, and fears."

	"You cannot mandate trust and integrity, and you cannot put it out in a policy statement. It is often a relationship based on communication." "The organization has to model the appropriate and fair behaviors in the program that the policy talks about."