The Cybersecurity Readiness Podcast Series

Episode Title	Stopping Social Engineered Vishing Attacks Before They Start
Podcast Series	The Cybersecurity Readiness Podcast Series https://www.cybersecurityreadinesspodcast.com/
Host and Producer	Dave Chatterjee, Ph.D. https://dchatte.com
Guest	Richard Quattrocchi, Vice President of Digital Transformation, Mutare Inc.
Summary Pitch	Social engineering continues to be the primary gateway for cyberattacks, responsible for nearly 80% of fraud and ransomware incidents. And notably, 1 in 4 of these social engineering attacks originate via phone calls. Yet many enterprises continue to leave their phone systems exposed. In this episode, Dr. Dave Chatterjee engages Richard Quattrocchi, Vice President of Digital Transformation, Mutare Inc., in a compelling discussion on the often-overlooked threat of voice-based cyberattacks, particularly vishing (voice phishing). Richard shares his professional journey, personal motivation rooted in a family scam incident, and the alarming rise of social engineering via phone calls—especially in the era of AI and deepfakes. The conversation underscores how organizations continue to leave phone systems vulnerable due to siloed ownership and outdated assumptions. Richard presents a layered defense strategy combining people, process, and technology, and introduces Mutare's voice traffic filtering solution. This technology proactively intercepts malicious calls using metadata analysis before they reach users, drastically reducing exposure to fraud. The discussion also dives into real-world cases, including the MGM

	breach, and offers actionable guidance for enterprises and individuals to better secure voice channels.
Action Items and Discussion Highlights	**Enterprise-Level Actions**: • Acknowledge the voice channel as a threat vector. • Break down organizational silos between telecom, IT, and security teams. • Implement layered defenses using people, process, and technology. • Use metadata-driven call screening (e.g., Mutare’s voice traffic filter). • Leverage CAPTCHAs for suspicious calls to thwart auto-dialers. • Tailor implementation to specific industry needs (healthcare, finance, etc.). • Ensure cross-functional governance and “do no harm” deployment. • Align with SEC’s ‘reasonable measures’ expectations for cyber risk management. **Individual-Level Actions:** • Use premium call-blocking apps (e.g., Nomorobo, Robokiller). • Don’t answer unknown or “spam risk” calls. • Verify requests by independently calling back known contact numbers. • Be skeptical and validate identity, even with familiar voices.
Time Stamps	• **[0:49] Introduction** o Dave introduces the episode's focus on voice channel vulnerabilities in cybersecurity. • **[1:41] Guest Introduction**

	○ Richard shares his background and personal connection to voice-based cyberattacks. • **[4:35] Personal Experiences with Vishing** ○ Both speakers recount personal stories of elder relatives being targeted via social engineering. • **[7:29] Why Voice Is a Blind Spot** ○ Organizational silos and legacy views leave voice systems unprotected; deepfakes worsen the risk. • **[11:53] MGM Voice Phishing Case Study** ○ A 10-minute vishing call led to a $300M+ incident—Richard explains how it unfolded and how it could’ve been prevented. • **[16:14] Human Factors in Cybersecurity** ○ Discussion on how human psychology can override technical defenses, emphasizing layered security. • **[19:14] People-Process-Technology Approach** ○ Importance of integrating process discipline with security technology to reduce human error. • **[20:14] Mutare's Voice Traffic Filter Technology** ○ Richard describes a metadata-driven solution that blocks malicious voice calls pre-ring, preventing social engineering at the outset. • **[24:36] Protecting Seniors in Elder Communities** ○ Real-world example: how Mutare’s solution completely blocked scam calls in a senior living facility. • **[27:35] Seamless Enterprise Implementation**

	○ Tailored deployment strategies ensure legitimate calls are preserved while malicious ones are filtered. • **[31:07] The Need for Cross-Functional Collaboration** ○ Success requires coordination between security, IT, telecom, and leadership. • **[34:04] Legal Implications and SEC Mandates** ○ SEC requires public companies to take reasonable cybersecurity measures—failure may result in lawsuits (e.g., MGM). • **[35:36] Takeaways for Security Professionals** ○ Acknowledge the voice threat, treat cybersecurity as a strategic investment, and foster cross-functional governance. • **[38:37] Advice for the General Public** ○ Use call blockers, don't trust unsolicited calls, and always verify by calling back known numbers.
Memorable Richard Quattrocchi Quotes/Statements	"When it comes to social engineering, which is one of the things we're going to talk about today, and the attacks that happen, it's best to stop them by using what I'd call an in-depth layer of defense approach." "The biggest reason, voice remains a blind spot in enterprise security is because organizational silos and what I call digital tunnel vision have left it behind." "Most cybersecurity investments prioritize email, endpoints, cloud systems, while voice, despite being heavily exploited in social engineering, falls outside the typical security stack." "Everybody puts a firewall in front of their email system to stop the spam. They're putting nothing in front of that voice channel."

	“MGM is the poster child for socially engineered voice phishing.” “When you think of these attacks, this is not the kid in a hoodie in the basement. This is organized crime. I was looking at a photo the other day the FBI provided for me of a building in Myanmar. 500 employees come to work every day, working the phones, and they're doing scams, from the grandma scam that I talked about earlier, about my mother, all the way through to enterprise scams where they are impersonating the CEO.” “Securing the voice channel isn't just about blocking bad calls, it's about doing it in a way that's seamless, that’s responsible, and it's tailored, and this is the most important part to the organization's unique environment.”