The Cybersecurity Readiness Podcast Series

Episode Title	Lessons from 2024's Biggest Cyber Incidents and Building Stronger Defenses for 2025
Podcast Series	The Cybersecurity Readiness Podcast Series https://www.cybersecurityreadinesspodcast.com/
Host and Producer	Dave Chatterjee, Ph.D. https://dchatte.com
Guest	Shrav Mehta, Founder and CEO at Secureframe
Summary Pitch	Dr. Dave Chatterjee and Shrav Mehta discuss major cybersecurity incidents in 2024, highlighting five significant breaches: National Public Data (2.7 billion records), AT&T (50 billion), Ticketmaster (500 million), Change Healthcare (145 million), and Dell (49 million). They emphasize the importance of proactive measures, such as data minimization, continuous training, and zero-trust models. Dr. Chatterjee stresses the need for leadership engagement, robust incident response plans, and a holistic approach to security. Mehta underscores the role of automation and continuous monitoring in enhancing security. Both agree on the necessity of evolving security practices to counter emerging threats like deepfakes and AI-enabled attacks.
Action Items and Discussion Highlights	▪ Review and strengthen the organization's security awareness training program to address evolving threats like deepfakes. ▪ Implement robust multi-factor authentication methods and explore using cryptography and biometrics for identity verification. ▪ Regularly stress test the organization's incident response plan through simulations and drills. ▪ Ensure basic security controls are in place, such as role-based access, secure password policies, and endpoint security.

	▪ Foster a cybersecurity culture by building emotional capital, ensuring leadership commitment, and making security everyone's responsibility.
Time Stamps	00:02 – Introduction 02:17 – Guest's professional highlights 03:05 – 2024 Breach Report Highlights 05:36 – Common Organizational Vulnerabilities and Weaknesses 09:41 – Getting Cybersecurity Right 16:38 – Holistic Approach to Cybersecurity 22:16 – Driving a Culture of Security 25:06 – Best Practices 29:13 – Zero Trust Security Model 30:56 – Creating a "We-Are-In-It-Together" Culture and Building Emotional Capital 33:45 – Closing Thoughts
Memorable Shrav Mehta Quotes/Statements	"When you review data breach incidents, it's almost never the case where some sophisticated hacker breaks through a robust defense system. I don't think I've seen a case like that in ages. It's usually something simple where the perpetrator takes advantage of scenarios such as encryption being weak or non-existent, or multifactor authentication is not enabled." "You can't use sampling methodologies to test and ensure compliance."

	"Oftentimes, the weakest link in your supply chain is a smaller company, and if that company has access to a lot of your data, they need to be just as secure. And honestly, that's where attackers are looking, the weakest link in your supply chain. "More than just training the humans, we need better software, better tooling to determine when an attack is happening." "Make sure that you have internal policies for business continuity, stress testing, secure passwords, multifactor authentication, end-point security, and employee security awareness training. These are some of the really basic things." "It is very important for leaders to set the foundation and ensure transparency across the board. "Make sure that you're prepared and have all the basics checked. Make sure that you're following some sort of security framework at a minimum, like SOC II, or ISO 27001 or some of the NIST standards, whatever is most applicable to your company. I think it's really important that there is some sort of continuous monitoring, and that you're always evolving your security program with the latest threats and attack vectors that are out there."