

The Cybersecurity Readiness Podcast Series

Episode Title	Role of Top Management in Cybersecurity Governance
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	Rohit Verma, CEO of Crawford and Company
Summary Pitch	<p>The recent ransomware attacks on Colonial Pipeline and JBS are grave reminders that organizations at all levels must constantly be in a high state of cybersecurity readiness and alert. This is no easy task as the points of vulnerabilities are numerous, especially the probability of humans falling prey to innovative hacking maneuvers. The senior leadership has an incredibly important and critical role to play in securing operations, sensitive data, and other digital assets. They must actively engage in the planning and execution of cybersecurity governance activities and spearhead the creation and sustenance of a high-performance information security culture. Such a high-performance information security culture is anchored on three key pillars – commitment, preparedness, and discipline. Dr. Dave Chatterjee’s book on Cybersecurity Readiness: A Holistic and High-Performance Approach speaks to these security culture traits and associated success factors. Probably the most important success factor is a highly committed and engaged top management. In an extensive and insightful discussion with Dr. Chatterjee, Rohit Verma, CEO of Crawford and Company, speaks candidly on topics ranging from top management involvement to the empowerment of the Chief Information Security Officer (CISO), cyber training and assessment, intelligence monitoring, performance tracking and measurement, security drills, and best practices. The following are some memorable Rohit</p>

	Verma quotes as he advocates a genuinely committed approach to cybersecurity readiness.
Time Stamps	<p>02:30 – What according to you should be the nature and extent of top management involvement in cybersecurity governance?</p> <p>04:35 – How do you approach cybersecurity readiness from a strategic standpoint?</p> <p>06:27 – Is there any particular cybersecurity performance metric or key performance indicator that you track as an organization?</p> <p>07:49 – How does your organization strive to raise the cybersecurity knowledge and skill level among all employees?</p> <p>11:59 – How does your company process the cyber intelligence they receive?</p> <p>16:11 – In a company like yours which is globally dispersed, it is not easy to institute and manage cybersecurity initiatives. What are some of the challenges you encounter doing that and how do you work through them?</p> <p>18:03 – Now talking about Chief Information Security Officer (CISO), a thought that came to mind, is how do you empower the CISO function?</p> <p>20:56 – What advice do you have for senior leadership for other organizations that may not be as committed to regularly updating their cybersecurity knowledge levels?</p> <p>27:40 – Do you have any final words for our listeners?</p>

Rohit Verma's Memorable Quotes/Statements	<p>“Approach cybersecurity at work with the same genuineness and care as you would when securing your own home and family.”</p> <p>If the leadership of other organizations needs any convincing about staying up with cyber training, all they need to do is look up the WSJ for the last three months and read about the extent of havoc cybersecurity can cause an organization. The cost of recovering from the attack is quite significant. Clearly, “prevention is better than cure.”</p> <p>“Several of us in senior leadership are digital immigrants and not digital natives. Many of the security issues are new to us. We will be naïve if we don't take interest and are not willing to learn and stay updated.”</p>
--	--