The Cybersecurity Readiness Podcast Series

Episode Title	Securing the Smart Supply Chain
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	Alan Mihalic, President IoT Security Institute
Summary Pitch	In episode 18, Alan Mihalic, President IoT Security Institute, speaks to the challenges and success factors associated with securing Internet-of-Things (IoT) devices in smart supply chains. He draws upon the IoT Security Framework to share some guiding principles and practices to help supply chain participants specify, procure, install, integrate, operate, and maintain IoT securely for smart cities and critical infrastructure.
Time Stamps	00:42 -- Please share with the listeners a bit about your cybersecurity journey? 02:17 -- How would you define or describe the challenges of a smart supply chain? 06:56 -- In fact, you mentioned during our prior discussion about the security-by-design approach, and that really appeals to me, I'd love for you to expand on that for our listeners. 14:22 -- What are your thoughts and recommendations on vendor selection and vendor management in the context of IoT devices? 29:20 -- Can you speak about the IoT Security Institute, its offerings, and its benefits?

	40:57 -- I'd like to give you the opportunity to close it out with some key messages for our listeners.
Memorable Alan Mihalic Quotes/Statements	06:17 So to protect a smart grid or water supply or things of that nature, the government can't just do it, the government relies on the community and corporations to ensure they do their part. Now, that ostensibly may seem a very logical thing and it certainly is, but from a practical deployment and accountability perspective, it is a seismic shift in the way we look at security. 13:27 The underpinning success story of any smart technology implementation is to trust more. We can stand up a server if it gets knocked out, we can stand up a power plant if it gets knocked down, but when the trust of the community is knocked over, then that's a very hard thing to get back. 14:06 It's very hard to ask someone to provide all the privacy information, all of the access to things that can be aggregated and circulated when that's abused. 17:20 IoT device has to fit be fit for purpose, it needs to be able to maintain baseline security that is in accordance with the data that it's collecting, aggregating, filtering, analyzing, etc. It cannot simply be a dumb device, for want of a better word, that has no inherent security controls. 17:47 You could spend an awful lot of money on security controls, but be undermined and done in by a $10 IoT device.