The Cybersecurity Readiness Podcast Series

Episode Title	A Deep Dive into Ransomware Attacks and Negotiations
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	Art Ehuan, Vice President, Palo Alto Networks, and Former FBI Special Agent
Summary Pitch	Art Ehuan, Vice President, Palo Alto Networks, and Former FBI Special Agent, discusses at length the unfortunate evolution and escalation of ransomware attacks. He explains how the threat actors have upped their game and are now engaging in double, triple, and quadruple extortions. While lamenting that "organizations continue to make the same mistakes," Art also acknowledges the challenges of vulnerability management. He offers some interesting insights into ransomware negotiations and provides excellent advice and recommendations on how to proactively thwart such attacks.
Time Stamps	03:00 Before we started the recording, you made a statement that "companies keep making the same mistakes." Tell us more about it. 07:03 For the benefit of our listeners, if you would explain what a ransomware attack is and what the threat landscape is like? Who are the threat actors? 10:57 What is the level of preparedness?

	15:20 Have you seen any best practices out there or any exemplars where irrespective of the directive, irrespective of board oversight, there is a conscious commitment to create and sustain a high-performance information security culture? Have you seen evidence of that? 22:01 I have seen a difference between having frameworks and truly following the framework in a very disciplined and committed manner. And there being some oversight to ensure that the compliance is thorough, the compliance is meticulous. What have you seen? 25:28 Please provide some insights into ransomware negotiations. 31:32 What is the best defense against ransomware attacks? And you've already shared with us that, patch management is important, but that can be challenging. What else? What else should companies be doing to reduce the possibility of such attacks? 35:06 Have you come across an instance where a company was a victim of a ransomware attack and they're like, "doesn't matter, thank you very much, we are all backed up and good to go?" 38:54 I've also heard that if you (organization) pay, you are on that list. And they (threat actors) know that if you are attacked again, you will pay again. Is that true? 39:35

	We are aware of the Colonial Pipeline attack, and how the FBI was able to recover some of the ransom money. Given your experience with the FBI, why is it so hard to get hold of these criminals, and put them away? 41:05 If crypto could be regulated, that might help mitigate some of these types of attacks? Do you have any thoughts on that? 44:17 What are your thoughts on senior leadership treating cybersecurity as a strategic priority, as a distinctive competency, and making every effort to protect against all possible vulnerabilities? 48:03 There might come a time, hopefully, sooner than later, when the CISO reports directly to the Board? This would allow the CISO function to operate as independently as possible. Your thoughts? 53:44 I would like you to wrap it up for us with some final words.

Memorable Art Euhan Quotes/Statements	The importance of hygiene around patch management -- making sure that you've got a vulnerability management program, and that you implement it so that as vulnerabilities are identified on systems, you're patching them in a timely fashion. You could potentially have a nation-state masking their activity as a ransomware attack when they're actually burrowing into your infrastructure. You're (CEO) trying to make a determination, do I put more money into cyber, or do I put more money into customer satisfaction? You know, that's sometimes a hard decision because you've got limited dollars, and trying to make that decision is sometimes difficult? If you're the CEO, you want to do the right thing, make sure the company is protected. But you also want to make sure that your customers are happy and you're doing everything possible to provide those products or services. So, sometimes that's a very difficult balancing act. If you're just checking a box, you're not meeting the spirit of the framework, you're not actually doing what you really need to be doing to ensure the security of the organization. There is this view out there, that if we pay and get the key, the next day, we're up and back in operation. I want to dispel that myth that you get the key and you're back in operation the next day. It typically is going to take several days, even when you get the key. One of the first things that these threat actors do when they get into the environment is go looking for the backups because those are going to be some of the first systems they hit you with ransomware attacks. They're going after the backups. It is very difficult for an organization to say to their C-level or their board, hey, I absolutely 100% guarantee we will never suffer a breach. But you can do things to minimize impact. Or, even better, make it hard for that group or

	that attacker. Make it so hard that they're just going to move on to another company. If you pay, the threat actor group will follow through with what they've promised to you. Right now, the deterrence factor, unfortunately, is very low. Because it's very difficult to have these individuals (threat actors) arrested. Ransomware is more than just a CISO problem. It's a corporate problem. You need the executives, you need the Board, you need the executives, you need the management, and you need the employees to all to be in unison, in how do we protect our company? I'm a huge fan of anything that will get the CISO as close to the CEO, or the Board as possible so they can have that influence.