The Cybersecurity Readiness Podcast Series

Episode Title	The Last Line of Defense Against a Ransomware Attack
Podcast Series	The Cybersecurity Readiness Podcast Series https://www.cybersecurityreadinesspodcast.com/the-last-line-of-defense-against-a-ransomware-attack/ https://www.cybersecurityreadinesspodcast.com/
Host and Producer	Dave Chatterjee, Ph.D. https://dchatte.com
Guest	Gabe Gambill, VP of Product and Technical Operations at Quorum
Summary Pitch	Attackers have started increasingly targeting victims' backups to prevent organizations from restoring their data. Veeam's "2023 Ransomware Trends Report" found more than 93% of ransomware attacks specifically targeted backup data. My discussion with Gabe Gambill, VP of Product and Technical Operations at Quorum, revolves around the following questions: • What vulnerabilities of data backups do ransomware hackers exploit? • What are the common mistakes and barriers when recovering against a ransomware attack? • How to successfully recover from a ransomware attack?
Time Stamps	00:02 -- Introduction 00:49 -- Setting the Stage and Context for the Discussion 01:41 -- Guest's Professional Highlights

	02:16 -- Revisiting Ransomware Attacks 03:24 -- Phishing, the Primary Delivery Method for Ransomware 04:33 -- Ransomware Attack Statistics 05:34 -- Payment of Ransom 06:51 -- Protecting and Defending from Ransomware Attacks 08:07 -- Franchising Ransomware 08:51 -- Last Line of Defense against a Ransomware Attack 10:23 -- Data Backups and Prioritization 11:33 -- Data Recovery Best Practices 13:31 -- Holistic Approach to Tabletop Exercises 14:40 -- Significance of Practicing the Data Recovery Process 14:48 -- Common Mistakes and Barriers when Recovering from a Ransomware Attack 18:47 -- Being Appropriately Prepared For Disaster Recovery 20:38 -- Vulnerability Management 21:37 -- Reasons for Not Being Proactive 24:48 -- CISO Empowerment 25:54 -- Cross-Functional Involvement and Ownership 26:56 -- CISO as a Scapegoat 28:43 -- Multi-factor Authentication 29:47 -- Best Practices to Recover from Ransomware Attacks 31:26 -- Final Thoughts

Memorable Gabe Gambill Quotes/Statements	"The next logical step was ransomware, where they're taking your data, and they're literally encrypting it right from under your nose and holding you accountable, so that they can get money out of you to give you back your own data." "More people are paying and not talking about it, which is the worst thing you can do in that situation." "80% of people that are hit with ransomware are hit again. So if I'm the ransomware person, who am I going to attack? I'm going to attack Caesars Palace (hotel in Las Vegas) again, I know they're going to pay. So there's the trade off there between the right thing to do and the hard thing to do." "The last line of defense are your backups. So it's like an onion, you're gonna have multiple layers of defense, you're gonna have security layers on your perimeter, you're gonna have antivirus, you're gonna have endpoint protection, you're gonna have things such as network scans. There's all kinds of things you can do to provide layers of protection into your environment." "The ransomware attack is not through vulnerabilities as much as through phishing. And because of that, people are the weakest link in your security plan, inevitably, it's going to happen to everybody." "The most common thing that I've found is when they recover from ransomware, they don't contact their insurance first. And the bad part about that, whether you're going to pay whether you're not going to

	pay, if you didn't contact your insurance first, chances are, they're not going to pay you back." "The other big mistake I see is people rushing the recovery to get back online versus getting back online safely." "On the technical side, the mistakes that I often see people make is they want everything to be integrated and simple. And there is a level for that in your production environment that is necessary. You need a domain, you want single sign-on, you want all of these things. In your backups, you want none of that you want Zero Trust, because that's the piece that has to recover when all the rest of it's dead." "They don't train enough. They have one training video that they've been spinning out for five years. Continuous training is very critical." "I've gone in with the Disaster Recovery (DR) manual and set it on the desk and had the white table discussion with customers. They don't do anything that's in their manual at all, just kind of winging it, as you said, Oh, we'll figure it out. And that's the way they treat the ransomware thing, even though they have a set of things of this is what you need to do; not following that ends hurting them." "Unpatched vulnerabilities is the second most common way that they (hackers) get into your environment." "One of the hardest things to implement in a company right now is multi-factor authentication, which sounds so silly because it's so popular, and everyone's doing it. But there's so many exceptions to the rule."

	"Ransomware is not a technical problem. And it should not be treated as a technical problem. It is a company wide problem. It needs to involve every level of the company, knowing how to respond, how to test, how to make those hard decisions, because they are very hard decisions when you're in the fire. And if you don't have some guidelines or some pre-selected things, chances are you'll make the wrong decision." "FBI and the CISA, which is the Central Intelligence Security Administration, have formed an international group to help fight ransomware that is starting to become very effective."