The Cybersecurity Readiness Podcast Series

Episode Title	How do SMBs protect themselves from ransomware attacks?
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	Grayson Milbourne, Security Intelligence Director at OpenText Security Solutions
Summary Pitch	A recent Global SMB Ransomware survey finds that nearly half of small and medium-sized businesses (SMBs) have experienced a ransomware attack, yet the majority aren't sure they are a target, and most are not confident they can fend off such an attack. Since 60% of SMBs are known to go out of business within six months of being hacked, it is a very troubling state of affairs. In this episode, Grayson Milbourne, Security Intelligence Director at OpenText Security Solutions, joins me in discussing the security challenges faced by SMBs and sharing success factors and best practices.
Time Stamps	02:21 -- Before we get into the details of SMB information security challenges and best practices, let's talk about you a bit. Share with listeners some highlights of your professional journey. 04:19 -- From a cybersecurity risk resiliency and defense standpoint, small and medium-sized businesses (SMBs) are often the most vulnerable and least mature. As one CIO of a midsize bank put it, "many cybercriminals are specifically targeting midsize companies that are in the cybercrime sweet spot. They are big enough to have significant bank accounts, but they often don't use the latest

	cybersecurity defenses. Also, middle market firms are often the gateway to bigger targets for cyber thieves." Your thoughts and reactions? 10:53 -- In a study that my colleague, Mike Benz and I published, we noted that 95% of the surveyed SME IT leaders believe they have an above-average security posture. And so the concern is when you think you are prepared, but actually, you are not, that is a bigger problem. Don't you agree? 17:38 -- Grayson, I'd like to go back to the ransomware report, the survey report that your organization published. It's concerning that nearly half of SMBs have experienced a ransomware attack. And yet the majority still don't think or aren't sure they are a target. Why don't you expand on this? 23:57 -- Grayson, what are the top three things that you would recommend SMBs do to protect themselves from, say, ransomware attacks, what would be those top three things? 30:43 -- My research finds that time, and again, a lot of planning happens, and a lot of documentation is maintained. But when it comes to execution, that's where organizations fail time and again. Your thoughts? 36:05 -- I'd like to give you the floor to wrap things up for us.
Memorable Grayson Milbourne Quotes/Statements	"What we see in the SMB spaces is that if they encounter ransomware, they don't report it. And they want to sweep it under the rug, move on and pretend it didn't happen. And unfortunately, that has other consequences that come along with it." "One of the biggest things that causes a headache during a ransomware incident is that it's a timed attack. They don't give you a lot of time to pay the ransom before they increase the demand because they know you're going to start scrambling, you're going to start thinking, Okay, what backups do I have in place? If you rehearsed the plan, at least you

	have a battle card to go to, you have some steps, and you're not scrambling because this is the worst time to be scrambling." "I think one thing that insurance probably doesn't look at is your readiness plan." "It comes down to reacting properly in that critical amount of time when you face one of these types of attacks." "Average downtime can be several weeks. It is right to look at cyber risk as any other risk to your business's continuity." "As your business grows, I think there's tremendous benefit in having an internal security-focused resource." "Ransomware reporting is vastly underreported. People don't want to have that black eye, they don't want to; it's bad for the customers. If it's not reported, it creates an even fuzzier picture for law enforcement that has resources to go after these organized groups." "The vast majority of attacks succeed because of a human error of somebody falling for something, clicking on a link, giving away too much information. And so I think education and awareness are really important." "It's a living and continuous cycle of identifying your assets, protecting them, detecting and looking for active infections, having a response plan in play, learning from your mistakes, and educating." "Having a plan is very different from having a fire drill with your plan." "If something bad happens, that's okay; come forth with the information and share it so that we can, as a community, defend ourselves better."