The Cybersecurity Readiness Podcast Series

Episode Title	Cybersecurity Risk Reduction Tips for Small and Medium Enterprises
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	Mike Benz, Partner | Fractional CIO at Fortium Partners
Summary Pitch	While small and medium-sized enterprises (SMEs) face the same cybersecurity issues as large enterprises, SMEs don't have the resources to effectively manage those risks. Research reports reveal alarming statistics on the state of cyber readiness of SMEs -- 60% of small businesses that are victims of a cyber attack go out of business within 6 months; 47% of small businesses have no understanding of how to protect themselves against cyber-attacks. Mike Benz, Partner | Fractional CIO at Fortium Partners, provides some useful tips on how SMEs can reduce their cybersecurity risk exposure without spending a fortune. Mike is the primary author of a scholarly publication Calculated Risk? A Cybersecurity Evaluation Tool for SMEs .
Time Stamps	2:07 – What is the state of cybersecurity readiness and needs in small and medium enterprises (SMEs)? 3:19 – What are some specific action items that you would recommend for SMEs? 5:01 – Don't you think asset identification and prioritization are key to managing cyber risks at SMEs?

	5:57 – How do you go about determining the risk tolerance levels of SMEs? 7:07 – How do you create a high-performance cybersecurity culture of commitment, preparedness, and discipline? 9:27 – What recommendations do you have for SMEs from the standpoint of systems monitoring? 12:14 – How should the SMEs plan for potential attacks? 16:04 – Please share how the cybersecurity evaluation tool (that you have developed) can help SMEs assess their cybersecurity governance maturity. 20:33 – What does it take to get senior leadership commitment to cybersecurity governance? 25:32 – Shouldn't companies go beyond table-top exercises when it comes to information security drills? 28:28 – My research finds (as described in the book) 17 success factors associated with different aspects of cybersecurity governance, a lot of things have to be in place and have to be done well to effectively secure an organization. Getting a grasp of all these different defense measures, and thereby create an effective defense-in-depth strategy, takes a certain amount of training, a certain amount of maturation, it takes time. Organizations need to engage in simulated exercises, have regular reviews, and that's how they get better at it. Thoughts? 32:03 – What advice do you have for SMEs in terms of identifying a reliable service provider? 38:27 – Any final thoughts?
Memorable Mike Benz Quotes/Statements	"Emergency responders such as fire departments know exactly how to handle a problem. They practice it all the time. I think SMEs should have a plan and practice that plan."

	"What we found was that most organizations didn’t need to hire a sophisticated consulting organization, or an army of security engineers, spend a fortune on state-of-the-art defenses, but they really needed to address cybersecurity in a fairly organized way." "Having business leaders recognize that cybersecurity risk is a business risk issue and not just an information technology issue is key."