The Cybersecurity Readiness Podcast Series

Episode Title	Securing SMBs serving Defense Industrial Base and U.S. Critical Infrastructure
Podcast Series	The Cybersecurity Readiness Podcast Series https://www.cybersecurityreadinesspodcast.com/
Host and Producer	Dave Chatterjee, Ph.D. https://dchatte.com
Guest	Chris Petersen, Co-Founder and CEO of RADICL
Summary Pitch	In this episode, Chris Petersen, Co-Founder and CEO of RADICL and I discuss the challenges of securing the small and medium-sized businesses (SMBs) that serve United States defense industrial base (DIB) and critical infrastructure. These SMBs play a major role in supporting the Advanced Defense Systems that keep our nation safe, both from domestic and international threats. So, it's imperative that we review what it takes to keep these SMBs safe from cyber-attacks. **Action Items and Discussion Highlights** • Treat cybersecurity as a strategic opportunity and invest adequate resources to build and sustain this competency. • Establishing fail-safe software development practices. • Software testing and rollout models must be continuously and rigorously tested. • Proactively determining different disaster scenarios and stress testing organizational resilience in dealing with those situations. • Consider establishing key metrics to measure the effectiveness and maturity of cybersecurity operations. • Demand visibility and transparency into the specific activities a managed service provider is conducting to protect the organization, such as vulnerabilities remediated, security incidents handled, and training completed. Regular reporting should be provided.

	• Conduct thorough due diligence when selecting a cybersecurity [1]service provider, including validating the qualifications and expertise of the individuals who will be responsible for security, the technologies used, and references from other customers.
Time Stamps	00:02 -- Introduction 02:09 -- Guest's Professional Highlights 04:32 -- Chris Petersen's Perspective on the Global IT Outage Fiasco 08:01 -- What could Delta have done differently? Could they have proactively predicted such a disaster scenario and prepared for it? 11:45 -- Key Findings from RADICL's 2024 DIB Cybersecurity Maturity Report 13:29 -- Chris Petersen's take on the survey findings 19:49 -- Recommendations on how SMBs serving the defense industrial base and critical infrastructure can meet and exceed compliance requirements. 24:21 -- Cybersecurity as a strategic opportunity 28:43 -- Guidance on selecting service providers and managing outsourced relationships 34:27 -- Advice for SMB CEOs 37:18 -- Closing Thoughts

Memorable Chris Petersen Quotes/Statements	"When we build software, our quality practices need to be fail-safe, especially when you have a footprint like CrowdStrike does that can be so impactful if there is an issue." "CrowdStrike needs to look at their testing model and perhaps their rollout model of how they roll out content updates." "Microsoft also shouldn't be so susceptible to a program operating in the kernel that can repeatedly cause a blue screen of death. There should be some resiliency built into the operating system itself." "I think the technology providers need to build more resiliency into their technologies, especially when they're foundational and are platform-level technologies. For security, folks need to make sure we are doing a really thorough job on the quality side." "I'm especially concerned because most of these companies typically don't have sophisticated incident response operations in place." "I'm concerned that these companies have accounts that have been compromised, have endpoints that have been compromised, but the vast majority of them don't have that class of forensic capability to detect and remove the malicious files." "The thing with compliance, though, is it comes down to how well you achieve compliance." "Fundamentally, business operations are going to trump security, because you have to do business." "The advice I'd give to a CEO is start thinking about establishing some operational metrics around security and the metrics that indicate you have some resiliency and defense-in-depth measures in place."