	- Cybersecurity investments should focus on process improvement rather than perfect outcomes. - Emotional narratives can drive decision-makers to act on cybersecurity risks. - Transparency about vulnerabilities encourages accountability and action. - Emotional appeals might oversimplify the complexity of cybersecurity, leading to misplaced priorities.
Why the Entire C-Suite Needs to Use the Same Metrics for Cyber Risk	- The lack of consistent cybersecurity metrics across the C-suite leads to misaligned priorities and weak risk management. - Common metrics like time-to-detect, breach costs, and downtime enable cohesive decision-making and better resource allocation. - Cybersecurity must be framed as a business risk rather than a purely technical issue. - Unified metrics improve coordination and accountability across leadership teams. - Clear, business-focused metrics ensure cybersecurity aligns with organizational goals. - Consistency in reporting strengthens overall risk management. - In my experience, putting too much weight on standardized metrics can oversimplify cybersecurity risks, often overlooking the unique and nuanced threats that vary from one industry to another.