1. Record Nr. UNINA9910826265403321

Autore	Hubbard Douglas W. <1962->
Titolo	How to measure anything in cybersecurity risk / / Douglas W. Hubbard, Richard Seiersen
Pubbl/distr/stampa	Hoboken, New Jersey : , : Wiley, , 2016 ©2016
ISBN	1-119-22461-6 1-119-22460-8 1-119-16231-9
Edizione	[1st edition]
Descrizione fisica	1 online resource (299 p.)
Collana	THEi Wiley ebooks
Classificazione	BUS061000COM053000
Disciplina	658.4/78
Soggetti	Cyberterrorism Cyberspace - Security measures Risk management
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	How to Measure Anything in Cybersecurity Risk; Contents; Foreword; Foreword; Acknowledgments; About the Authors; Introduction; Why This Book, Why Now?; What Is This Book About?; What to Expect; Is This Book for Me?; We Need More Than Technology; New Tools for Decision Makers; Our Path Forward; Part I Why Cybersecurity Needs Better Measurements for Risk; Chapter 1 The One Patch Most Needed in Cybersecurity; The Global Attack Surface; The Cyber Threat Response; A Proposal for Cybersecurity Risk Management; Notes; Chapter 2 A Measurement Primer for Cybersecurity; The Concept of Measurement Explaining the Elements of the Loss Exceedance CurveGenerating the Inherent and Residual Loss Exceedance Curves; Where Does the Risk Tolerance Curve Come from?; Supporting the Decision: A Return on Mitigation; Where to Go from Here; Notes; Chapter 4 The Single Most Important Measurement in Cybersecurity; The Analysis Placebo: Why We Can't Trust Opinion Alone; How You Have More Data Than You Think; When Algorithms Beat Experts; Some Research Comparing Experts and Algorithms; Why Does This Happen?; So What? Does This Apply to Cybersecurity?; Tools for Improving the Human Component

The Subjective Probability ComponentThe Expert Consistency Component; The Collaboration Component; The Decomposition Component; Summary and Next Steps; Notes; Chapter 5 Risk Matrices, Lie Factors, Misconceptions, and Other Obstacles to Measuring Risk; Scanning the Landscape: A Survey of Cybersecurity Professionals; What Color Is Your Risk? The Ubiquitous-and Risky-Risk Matrix; The Psychology of Scales and the Illusion of Communication; How the Risk Matrix Doesn't Add Up; Amplifying Effects: More Studies Against the Risk Matrix (As If We Needed More); Exsupero Ursus and Other Fallacies Beliefs about the Feasibility of Quantitative Methods: A Hard TruthSame Fallacy: More Forms; The Target Breach as a Counter to Exsupero Ursus; Communication and Consensus Objections; Conclusion; Notes; Part II Evolving the Model of Cybersecurity Risk; Chapter 6 Decompose It Unpacking the Details; Decomposing the Simple One-for-One Substitution Model; Just a Little More Decomposition; A Few Decomposition Strategies to Consider; More Decomposition Guidelines: Clear, Observable, Useful; Decision Analysis: An Overview of How to Think about a Problem; Avoiding "Over-Decomposition"
A Summary of Some Decomposition Rules

Sommario/riassunto

A ground shaking exposé on the failure of popular cyber risk management methods How to Measure Anything in Cybersecurity Risk exposes the shortcomings of current "risk management" practices, and offers a series of improvement techniques that help you fill the holes and ramp up security. In his bestselling book How to Measure Anything , author Douglas W. Hubbard opened the business world's eyes to the critical need for better measurement. This book expands upon that premise and draws from The Failure of Risk Management to sound the alarm in the cybersecurity realm. Some of the field's premier risk management approaches actually create more risk than they mitigate, and questionable methods have been duplicated across industries and embedded in the products accepted as gospel. This book sheds light on these blatant risks, and provides alternate techniques that can help improve your current situation. You'll also learn which approaches are too risky to save, and are actually more damaging than a total lack of any security. Dangerous risk management methods abound; there is no industry more critically in need of solutions than cybersecurity. This book provides solutions where they exist, and advises when to change tracks entirely. Discover the shortcomings of cybersecurity's "best practices" Learn which risk management approaches actually create risk Improve your current practices with practical alterations Learn which methods are beyond saving, and worse than doing nothing Insightful and enlightening, this book will inspire a closer examination of your company's own risk management practices in the context of cybersecurity. The end goal is airtight data protection, so finding cracks in the vault is a positive thing—as long as you get there before the bad guys do. How to Measure Anything in Cybersecurity Risk is your guide to more robust protection through better quantitative processes, approaches, and techniques.