1. Record Nr. UNINA9910713827803321

Autore	Hubbard Douglas W. <1962->
Titolo	How to Measure Anything in Cybersecurity Risk / / Douglas W. Hubbard and Richard Seiersen
Pubbl/distr/stampa	Wiley-Blackwell Hoboken, NJ : , : John Wiley & Sons, Inc., , [2023] ©2023
ISBN	1-119-89232-5 1-119-89231-7
Edizione	[Second edition.]
Descrizione fisica	1 online resource (366 pages)
Disciplina	658.478
Soggetti	Cyberspace - Security measures Cyberterrorism Risk management
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Cover -- Title Page -- Copyright Page -- Contents -- Foreword for the Second Edition -- Acknowledgments -- Preface -- How to Measure Anything in Cybersecurity Risk -- Introduction -- Why We Chose This Topic -- What Is This Book About? -- We Need More Than Technology -- Part I Why Cybersecurity Needs Better Measurements for Risk -- Chapter 1 The One Patch Most Needed in Cybersecurity -- Insurance: A Canary in the Coal Mine -- 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 -- A Taxonomy of Measurement Scales -- The Object of Measurement -- The Methods of Measurement -- Notes -- Chapter 3 The Rapid Risk Audit: Starting With a Simple Quantitative Risk Model -- The Setup and Terminology -- The Rapid Audit Steps -- Some Initial Sources of Data -- The Expert as the Instrument -- Supporting the Decision: Return on Controls -- Doing "Uncertainty Math" -- Visualizing Risk With a Loss Exceedance Curve -- 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 -- Tools for Improving the Human 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 -- Exsupero Ursus and Other Fallacies -- 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.
More Decomposition Guidelines: Clear, Observable, Useful -- A Hard Decomposition: Reputation Damage -- Conclusion -- Notes -- Chapter 7 Calibrated Estimates: How Much Do You Know Now? -- Introduction to Subjective Probability -- Calibration Exercise -- More Hints for Controlling Overconfidence -- Conceptual Obstacles to Calibration -- The Effects of Calibration -- Beyond Initial Calibration Training: More Methods for Improving Subjective Judgment -- Notes -- Answers to Trivia Questions for Calibration Exercise -- Chapter 8 Reducing Uncertainty with Bayesian Methods -- A Brief Introduction to Bayes and Probability Theory -- An Example from Little Data: Does Multifactor Authentication Work? -- Other Ways Bayes Applies -- Notes -- Chapter 9 Some Powerful Methods Based on Bayes -- Computing Frequencies with (Very) Few Data Points: The Beta Distribution -- Decomposing Probabilities with Many Conditions -- Reducing Uncertainty Further and When to Do It -- More Advanced Modeling Considerations -- Wrapping Up Bayes -- Notes -- Part III Cybersecurity Risk Management for the Enterprise -- Chapter 10 Toward Security Metrics Maturity -- Introduction: Operational Security Metrics Maturity Model -- Sparse Data Analytics -- Functional Security Metrics -- Functional Security Metrics Applied: BOOM! -- Wait-Time Baselines -- Security Data Marts -- Prescriptive Analytics -- Notes -- Chapter 11 How Well Are My Security Investments Working Together? -- Security Metrics with the Modern Data Stack -- Modeling for Security Business Intelligence -- Addressing BI Concerns -- Just the Facts: What Is Dimensional Modeling, and Why Do I Need It? -- Dimensional Modeling Use Case: Advanced Data Stealing Threats -- Modeling People Processes -- Conclusion -- Notes -- Chapter 12 A Call to Action: How to Roll Out Cybersecurity Risk Management -- Establishing the CSRM Strategic Charter.
Organizational Roles and Responsibilities for CSRM -- Getting Audit to Audit -- What the Cybersecurity Ecosystem Must Do to Support You -- Integrating CSRM with the Rest of the Enterprise -- Can We Avoid the Big One? -- Appendix A Selected Distributions -- Distribution Name: Triangular -- Distribution Name: Binary -- Distribution Name: Normal -- Distribution Name: Lognormal -- Distribution Name: Beta -- Distribution Name: Power Law -- Appendix B Guest Contributors -- Decision Analysis to Support Ransomware Cybersecurity Risk Management -- Bayesian Networks: One Solution for Specific Challenges in Building ML Systems in Cybersecurity -- The Flaw of Averages in Cyber Security -- Botnets -- Password Hacking -- How Catastrophe Modeling Can Be Applied to Cyber Risk -- Notes -- Index -- EULA.