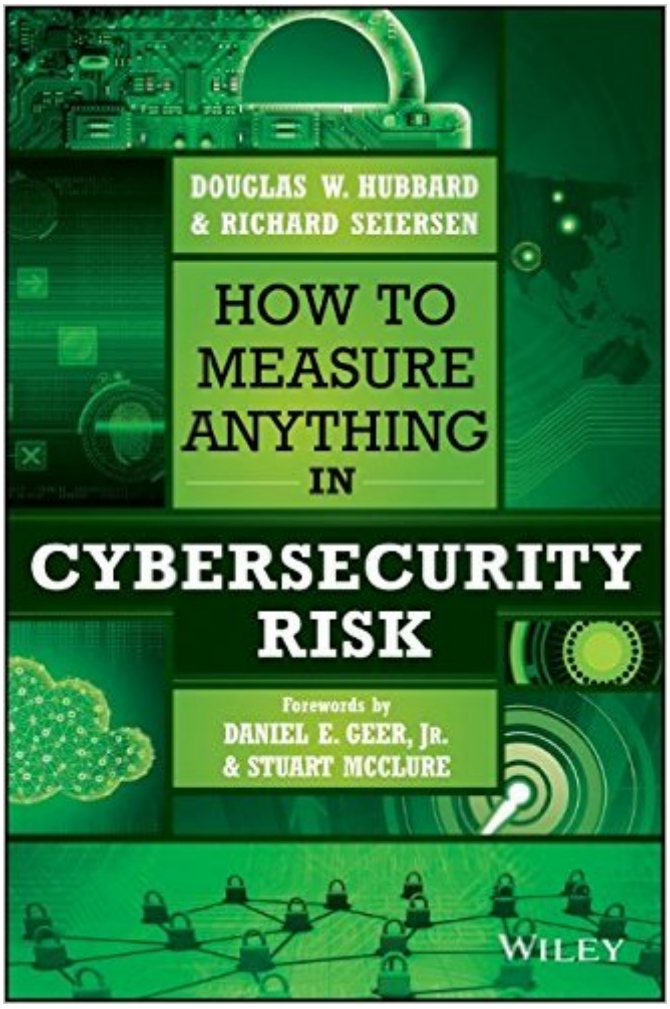
How To Measure Anything In Cybersecurity Risk



Synopsis

A ground shaking exposÃ© 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.Â 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 thingâ "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.

Book Information

Hardcover: 304 pages

Publisher: Wiley; 1 edition (July 25, 2016)

Language: English

ISBN-10: 1119085292

ISBN-13: 978-1119085294

Product Dimensions: 6.3 x 1 x 9.3 inches

Shipping Weight: 1.1 pounds (View shipping rates and policies)

Average Customer Review: 4.8 out of 5 starsÂ Â See all reviewsÂ (9 customer reviews)

Best Sellers Rank: #79,467 in Books (See Top 100 in Books) #94 inÂ Books > Business & Money

> Education & Reference > Statistics #176 inÂ Books > Science & Math > Mathematics > Applied > Statistics #230 inÂ Books > Computers & Technology > Security & Encryption

Customer Reviews

This book is a major contribution to our understanding of this critical subject. The main idea is that the biggest risk in cybersecurity risk assessment is reliance on ineffective methods, often because people don’t believe quantitative forecasts will work and then, when they do use quantitative estimates, don’t track them to see how well they do.. This echoes Hubbard’s reasoning about financial forecasts in The Failure of Risk Management; he has more data to back him up now.While readers familiar with Hubbard’s earlier work will find some repetition of what they know in the first half of the book, it is still worthwhile even for them. Hubbard has expanded and refined his treatment of his inventions, calibration and Applied Information Economics, and added examples. There is also a new presentation, in Chapters 8 and 9, of Bayesian inference, with a number of references to real-life applications. Chapters 10 through 12, which I surmise were largely written by cybersecurity expert Richard Seiersen, are excellent.The authors’ outline of how to establish and manage a Cybersecurity Risk Management function in an organization, and what that functional unit should do, are well written, well reasoned, and cogent. He lays out the key areas of responsibility this function should include: review all major initiatives for technology risk; monitor and analyze existing controls investments; use proven quantitative methods to understand and communicate risk; maintain organizational risk tolerances in coordination with the chief financial officer, general counsel, and the board; manage and monitor exception-management programs that violate established risk tolerances; and maintain cyberinsurance policies, in conjunction with legal and finance.

How to Measure Anything in Cybersecurity Risk Measure Twice, Cut Once: Simple Steps to Measure, Scale, Draw and Make the Perfect Cut-Every Time. (Popular Woodworking) Measure for Measure (Arden Shakespeare: Second Series) Measure for Measure (Arkangel Shakespeare) How to Measure Anything: Finding the Value of ’Intangibles’ in Business The Feeling of Risk: New Perspectives on Risk Perception (Earthscan Risk in Society) Cybersecurity for Everyone: Securing your home or small business network Cybersecurity: Home and Small Business Essential Cybersecurity Science: Build, Test, and Evaluate Secure Systems Cybersecurity (Special Reports) Cybersecurity Leadership: Powering the Modern Organization Cybersecurity and Cyberwar: What Everyone Needs to Know ISO/IEC 31010:2009, Risk management - Risk assessment techniques Security Risk Management: Building an Information Security Risk Management Program from the

Ground Up COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance (GRC) Processes Global Risk Agility and Decision Making: Organizational Resilience in the Era of Man-Made Risk Advances in Heavy Tailed Risk Modeling: A Handbook of Operational Risk (Wiley Handbooks in Financial Engineering and Econometrics) Quantitative Risk Management, + Website: A Practical Guide to Financial Risk Operational Risk Management: A Complete Guide to a Successful Operational Risk Framework Project Risk Management Guidelines: Managing Risk in Large Projects and Complex Procurements