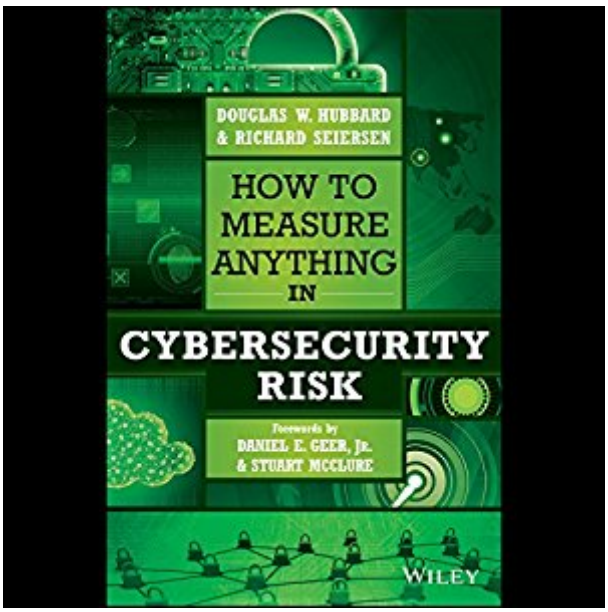
How To Measure Anything In Cybersecurity Risk



Synopsis

A ground shaking exposÃƒÆ'Ã Â© 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 best-selling 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.

Book Information

Audible Audio Edition
Listening Length: 10 hoursÃ Â andÃ Â 21 minutes
Program Type: Audiobook
Version: Unabridged
Publisher: Audible Studios
Audible.com Release Date: November 29, 2016
Language: English
ASIN: B01MXORDBA
Best Sellers Rank: #71 inÃ Â Books > Audible Audiobooks > Nonfiction > Computers #138

inÃ Â Books > Business & Money > Education & Reference > Statistics #182 inÃ Â Books > Computers & Technology > Security & Encryption

Customer Reviews

Absolutely essential for participants in any risk management program who want to get beyond faking things up with 3 level matrices. Quantitative risk analysis requires accuracy, but not absolute precision. This book gives great practical examples and training for getting to as much accuracy as you need for a given application. Study it, and make better decisions for your program.

Outstanding book. Walks you through going from qualitative assessments to applying quantitative rigor to cyber risk assessments. These methods (shown) brings cyber risk assessment and management more into conformance with standard risk management practices.

This book is a must-read for anyone trying to understand priority in Cyber Security operations. The authors take you through the basics of measurement, how risk has been misapplied in the cyber security industry, and makes recommendations for how to improve risk communication with executives. My favorite part is the discussion on Loss Exceedance Curves.

Hubbard should get a big ÃƒÂ¢Ã â ¬Ã Ëœthank youÃƒÂ¢Ã â ¬Ã â„¢ from everyone working in security and risk as his works are challenging the approach to risk management and improving quantitative risk and security thinking, metric generation and reporting. This is not a light read, but your invested time will be rewarded as your thinking is expanded and your skill set enriched.

Hubbard does a great job explaining how his technique can be applied to cyber security and the book is full of practical examples

This book is a must-read not only for cybersecurity professionals but also for data privacy professionals.The forward states that "you can’t manage something that you cannot measure." The book then goes on to evaluate traditional approaches to measuring cybersecurity risk, proposes improvements to such approaches and introduces more effective approaches and techniques.These approaches and techniques apply not only to "perimeter defenseÃƒÂ¢Ã â ¬Ã Â• mechanisms and ÃƒÂ¢Ã â ¬Ã Å“access controls" traditionally associated with cybersecurity ÃƒÂ¢Ã â ¬Ã â œ they also apply to data use issues associated with data privacy versus

cybersecurity. Recent changes in international data protection laws ÃƒÂ¢Ã â ¬Ã â œ which encompass both cybersecurity and data privacy ÃƒÂ¢Ã â ¬Ã â œ require that data be transformed into a ÃƒÂ¢Ã â ¬Ã Å“protect firstÃƒÂ¢Ã â ¬Ã Â• mode rather than remaining in "use first" mode where data remains vulnerable while in use.The new EU General Data Protection Regulation (GDPR) which goes into effect in 2018, and which includes fines of up to 4% of global revenues for infractions, calls this ÃƒÂ¢Ã â ¬Ã Å“protect first" mode "Data Protection by Default." Data Protection by Default under the GDPR requires that techniques be applied at the earliest opportunity (e.g., by pseudonymizing data at the earliest opportunity) so that data use is limited to the minimum extent and time necessary to support a specific product or service as expressly authorized by a data subject.Data Protection by Default and other ÃƒÂ¢Ã â ¬Ã Å“protect firstÃƒÂ¢Ã â ¬Ã Â• data protection regimes will require effective measurement of risks so they can be effectively implemented and managed. For these reasons, this book should be on the reading list of both cybersecurity as well as data protection professionals.

It’s essentially a rehash of his previous book. Not bad, but a rehash.That being said, the book is in my library and it does have useful new analytical material.Particularly good is the explanation of the notion that mostly everything is some measure of something. Case in point: in a recent meeting I asked my colleagues to rate something Low Mod High. Someone objected that that was ’so subjective’. My reply was Yes, but at least we will know what people think subjectively, and also - you know - we can train to be better estimators...it’s in the book and that’s a major contribution.So, like I wrote to Mr. Hubbard when he rightly pushed back on my original 3 stars / re-hash but good review, he’s correct: the book has a lot more than just a rehash; I stand corrected.

Ordered my mistake when looking for the title, but my graduate program cybersecurity statistics professor has read this book and HIGHLY recommends it for beginning researchers and interested minds!

Forensic Assessment of Violence Risk: A Guide for Risk Assessment and Risk Management How to Find Out Anything: From Extreme Google Searches to Scouring Government Documents, a Guide to Uncovering Anything About Everyone and Everything Cybersecurity for Beginners Cybersecurity Exposed: The Cyber House Rules Cybersecurity and Cyberwar: What Everyone Needs to Know Cybersecurity: Home and Small Business The Devil Inside the Beltway: The Shocking Expose of the US Government's Surveillance and Overreach Into Cybersecurity, Medicine and Small Business The Cybersecurity to English Dictionary Cybersecurity and Infrastructure Protection The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations Cybersecurity Ethics: An Introduction Cybersecurity (Special Reports)