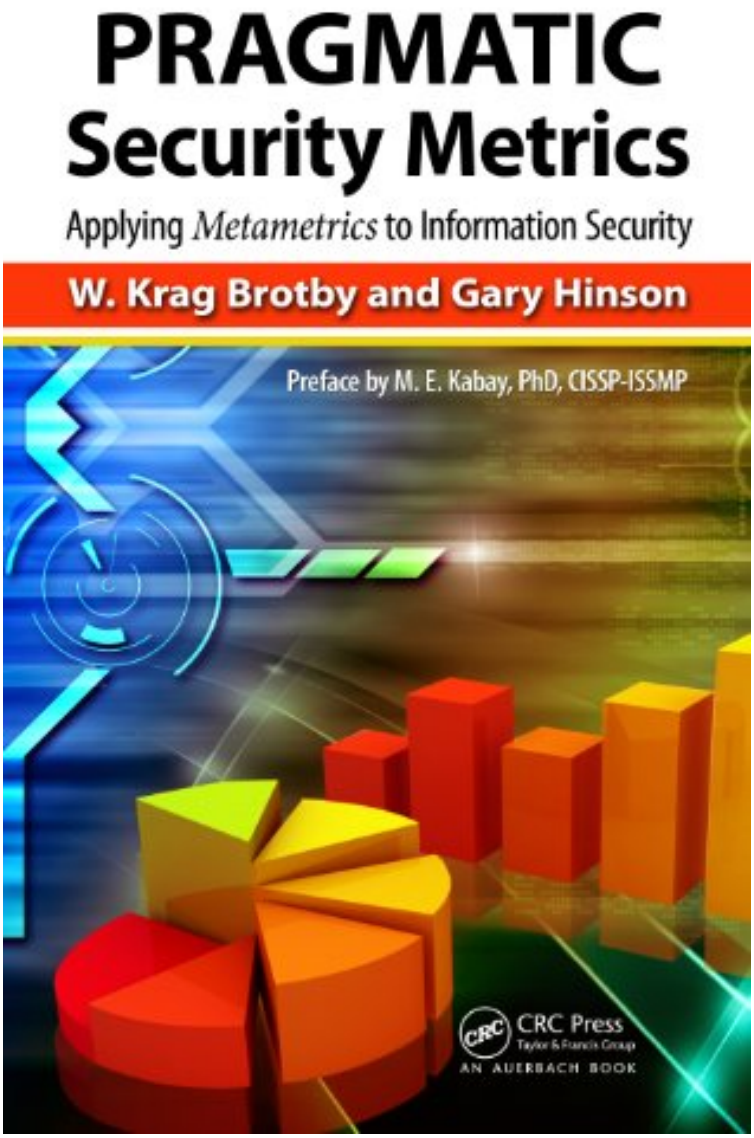
PRAGMATIC Security Metrics: Applying Metametrics to Information Security

W. Krag Brotby, Gary Hinson
*ebooks | Download PDF | *ePub | DOC | audiobook*



#584200 in eBooks 2016-04-19 2016-04-19File Name: B00CLZIKTK | File size: 49.Mb

W. Krag Brotby, Gary Hinson : PRAGMATIC Security Metrics: Applying Metametrics to Information Security before purchasing it in order to gage whether or not it would be worth my time, and all praised PRAGMATIC Security Metrics: Applying Metametrics to Information Security:

1 of 1 people found the following review helpful. Good for ALL metricsBy Patrick A. McCombsPRAGMATIC is an acronym for a set of meta-metrics. Addresses one of my major concerns, which is management demanding metrics just

because everyone else says metrics are good. Now you have a basis for evaluating metrics instead of just a gut feeling that "that's pointless." The book focuses on security metrics, and provides hundreds of examples, with PRAGMATIC scores. But the concept goes far beyond cyber security.1 of 1 people found the following review helpful. Outstanding bookBy RWalkerFantastic book on a vital subject for All Information Security and IT Risk Management practitioners1 of 1 people found the following review helpful. A must for anyone developing information security metricsBy SecureKatWell written and useful when developing information security metrics. The accompanying website and goodies were also very helpful. This one will join my permanent library.

Other books on information security metrics discuss number theory and statistics in academic terms. Light on mathematics and heavy on utility, PRAGMATIC Security Metrics: Applying Metametrics to Information Security breaks the mold. This is the ultimate how-to-do-it guide for security metrics.Packed with time-saving tips, the book offers easy-to-follow guidance for those struggling with security metrics. Step by step, it clearly explains how to specify, develop, use, and maintain an information security measurement system (a comprehensive suite of metrics) to help:Security professionals systematically improve information security, demonstrate the value they are adding, and gain management support for the things that need to be doneManagement address previously unsolvable problems rationally, making critical decisions such as resource allocation and prioritization of security relative to other business activitiesStakeholders, both within and outside the organization, be assured that information security is being competently managedThe PRAGMATIC approach lets you hone in on your problem areas and identify the few metrics that will generate real business value. The book:Helps you figure out exactly what needs to be measured, how to measure it, and most importantly, why it needs to be measuredScores and ranks more than 150 candidate security metrics to demonstrate the value of the PRAGMATIC methodHighlights security metrics that are widely used and recommended, yet turn out to be rather poor in practiceDescribes innovative and flexible measurement approaches such as capability maturity metrics with continuous scalesExplains how to minimize both measurement and security risks using complementary metrics for greater assurance in critical areas such as governance and complianceIn addition to its obvious utility in the information security realm, the PRAGMATIC approach, introduced for the first time in this book, has broader application across diverse fields of management including finance, human resources, engineering, and productionmdash;in fact any area that suffers a surplus of data but a deficit of useful information.Visit Security Metametrics. Security Metametrics supports the global community of professionals adopting the innovative techniques laid out in PRAGMATIC Security Metrics. If you, too, are struggling to make much sense of security metrics, or searching for better metrics to manage and improve information security, Security Metametrics is the place.http://securitymetametrics.com/

Like all books on metrics,nbsp;PRAGMATIC Security Metrics: Applying Metametrics to Information Security makes the statement that "you can't manage what you can't measure".nbsp; The authors claim that other books on information security metrics discuss number theory and statistics in academic terms. This title promises to be light on mathematics and heavy on utility and is meant as a how-to-do-it guide for security metrics.As to the title, PRAGMATIC is an acronym for the basis of the method of the book, in using metrics that are predictive, relevant, actionable, genuine, meaningful, timely, independent and cost. After reading the first chapter, PRAGMATIC Security Metrics: Applying Metametrics to Information Security looks like it may live up to its promise of being able to use metrics not only to track and report performance but to identify problem areas and opportunities, and drive information security improvements. If so, this could be the metrics book a lot of information security professionals have been waiting for.Ben Rothke, CISSP, CISM, Information Security Manager, Wyndham Worldwide; and author of Computer Security: 20 Things Every Employee Should Know, writing on the RSA Conference Blog, www.rsaconference.comAbout the AuthorKrag Brotbynbsp;CISM CGEIT has 30 years' experience in enterprise computer security architecture, governance, risk, and metrics. He is the principal author/editor of ISACA'snbsp;Certified Information Security Manager Manual, plusnbsp;Information Security Governance: Guidance for Boards of Directors and Guidance for Information Security Managers;nbsp;Information Security Management Metrics; and Information Security Governance: A Practical Development and Implementation Approach. nbsp;Krag has served on ISACA committees and the California High Tech Task Force Steering Committee, and frequently presents conference workshops and seminars. Krag was the principal architect for Xerox BASIA enterprise security and the SWIFT Next Gen PKI; served as technical director at RAND Corporation and chief security strategist for TransactPlus. nbsp;He developed policies for several U.S. banks and consulted fornbsp;Australia Post, New Zealand Inland Revenue, Singapore Infocom Development Agency, Microsoft, Unisys, ATT, BP Alyeska, Countrywide Financial, Informix, Visa, VeriSign, Digital Signature Trust, Zantaz, Bank Al-Bilad, J.P. Morgan Chase, KeyBank, Certicom, and Paycom, among others. nbsp;Krag delivers courses in metrics, governanceriskcompliance (GRC) and risk, and holds a foundation patent for digital rights management.Dr Gary Hinson PhD MBA CISSPnbsp;has worked in IT system and network administration, information security and IT auditing with multinationals in the pharmaceuticals/life sciences, utilities, IT, engineering, defense, and financial services industries, since the 1980s, and

consulting since 2000. His day job involves preparing security awareness materials for NoticeBored (NoticeBored.com), an innovative subscription service. nbsp;He is also responsible for ISO27001security.com, the ISO27k Toolkit and Forum supporting a global user community. Gary was originally a scientist researching bacterial genetics. The rational scientist and metrician still lurks deep within.