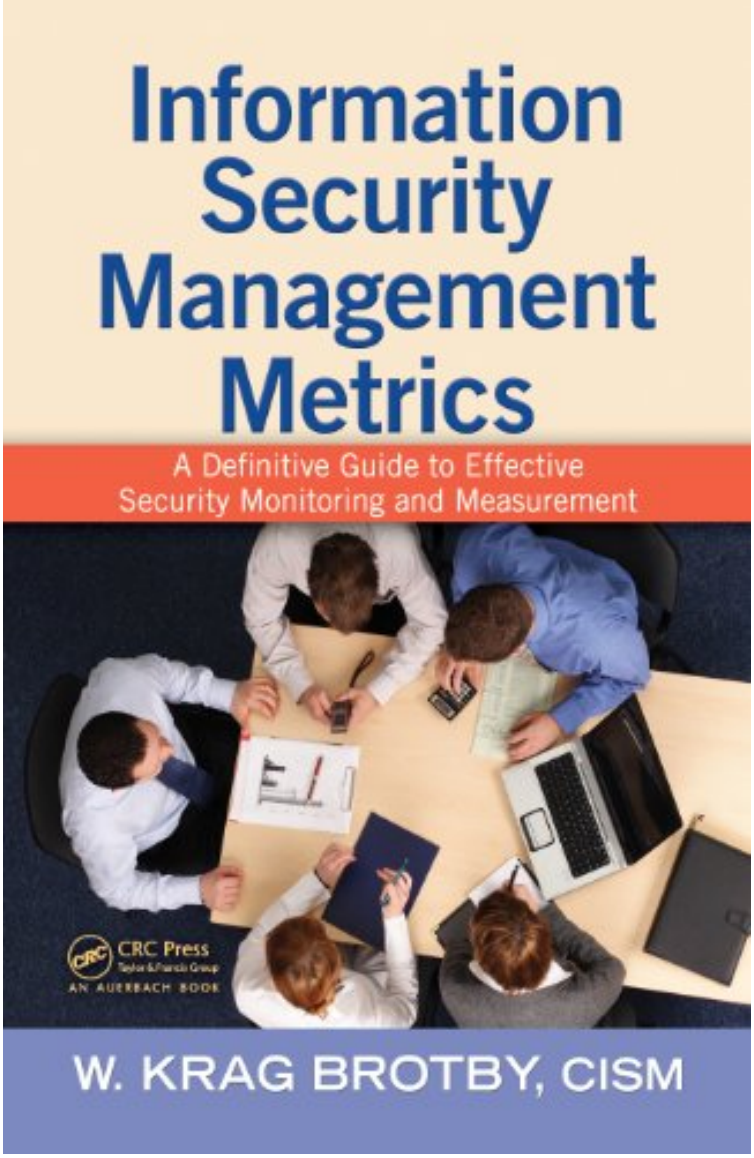
Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement

W. Krag Brotby CISM
**Download PDF | ePub | DOC | audiobook | ebooks*



#1556459 in eBooks 2009-03-30 2009-03-30File Name: B00AVA5LK8 | File size: 58.Mb

W. Krag Brotby CISM : Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement before purchasing it in order to gage whether or not it would be worth my time, and all praised Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement:

1 of 2 people found the following review helpful. High level collection of what's out in wildBy VPSAt the most, you can say that it's a good collection of what's out and about. Too much focus on few quantitative measures, and too little on 'Security metrics'.By no means it can be called "a definitive guide ...." It neither provides any ideas on 'monitoring' nor on real 'measurement metrics.'The index available as free download is misleading. It appears to cover a lot of ground and led me to purchase. However, if Goggling those topics or Wiki on any of those topics will provide more information than the narrative.I found the "Contents index" more useful than the book itself.5 of 7 people found the following review helpful. Conceptual framework for a tough topicBy Dr. G. HinsonMeasuring information security is the greatest remaining challenge for many of us. Metrics are essential for a scientific management approach, rather than relying purely on gut feel and guesswork. Standards such as ISO/IEC 27001 require the use of objective information about the status and effectiveness of information security controls in relation to the risks, in order to drive appropriate improvements in the Information Security Management System. However, it is not immediately obvious exactly what needs measuring, nor how to do it. This book lays out the foundations on which a rational measurement system can be designed to manage information security in a more objective fashion.The author encourages readers to consider a wide variety of measurement approaches and apply them sensibly to their information security management issues. In addition to conventional information security metrics, the book draws on governance, risk management, financial management and business analysis methods, a more diverse range of approaches than is normally covered in this field. Introducing measures of organization structure and culture sets this security metrics book apart from most others.Although the writing style is clear, this is a complex subject covered in depth. Being rather theoretical in approach, the book won't suit practitioners simply looking for a short checklist of `security things to measure'. However, those with the interest and time to study Information Security Management Metrics will be rewarded with a deeper and more rounded understanding of the issue. As such, the book is probably of most value to CISOs and ISMs tasked with implementing better security metrics, and to information security management students.1 of 2 people found the following review helpful. Think twice before buyingBy KoalaAs one reviewer noted, the coverage is very superficial. The book included some rather obscure models that I have never seen it used in the real world. Perhaps the book is simply mis-titled. For the practitioners in the field who read the book and start digging a little deeper, you'd get the sense that the author really didn't have much hands-on experience. One particular paragraph and chart caught my eye.Page. 68, the paragraph and chart on a study of the ROSI of various activities, based on a whitepaper from @Stake. The author provided no interpretation for the chart. The book claims it's based on an analysis of over 600 organisations. And wrote an insightful observation, "These results will undoubtedly be controversial and lead to energetic protests..." The following was what trouble me.Here is a short version of what the "saving to cost ratio" chart suggests: (1)Screen Locking has a 71.9% effectiveness in improving security; whereas things like (2) Nightly Back-up (only 0.2%) and (3) Central Access Control (0.1%). Firewall, IDS, patches...etc are in between (all below 10%)Any security professional who saw the chart and read the "insight" would question the findings and probably dig a bit deeper. I did. As it turns out, through a thin connection of mine who knows a guy who knows another guy who used to work for @Stake.They couldn't find any whitepaper on a ROSI study of 600+ organisations. (Doesn't mean it's not there, but he couldn't find it.)The cited source of the chart did worked for @Stake for a year or so. However, the chart actually came from the source's PhD thesis while he was an economic graduate at Stanford University. (I am actually reading his paper from my desktop as I type this) I am just going to copy the following verbatim, straight from the PhD thesis... in reference to the "saving to cost ratio" chart,"The savings were calculated by assuming that each safeguard was implemented in isolation."So.... how many of you implemented screen saver locking "in isolation" ? or turn on your nightly backup "only" and nothing else as a security measure ? Don't get me wrong, it was actually quite an interesting paper, well worth the read. I believe the paper actually got quite a bit of press coverage when it was first released.The only thing "controversial" about this is How did the author miss that ? (book author, not the original source)Two stars for the end of chapters References.

Spectacular security failures continue to dominate the headlines despite huge increases in security budgets and ever-more draconian regulations. The 20/20 hindsight of audits is no longer an effective solution to security weaknesses, and the necessity for real-time strategic metrics has never been more critical. Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement offers a radical new approach for developing and implementing security metrics essential for supporting business activities and managing information risk. This work provides anyone with security and risk management responsibilities insight into these critical security questions: How secure is my organization?How much security is enough?What are the most cost-effective security solutions?How secure is my organization?You canrsquo;t manage what you canrsquo;t measure This volume shows readers how to develop metrics that can be used across an organization to assure its information systems are functioning, secure, and supportive of the organizationrsquo;s business objectives. It provides a comprehensive overview of security metrics, discusses the current state of metrics in use today, and looks at promising new developments. Later chapters explore ways to develop effective strategic and management metrics for information security governance, risk management, program implementation and management, and incident management and

response. nbsp; The book ensures that every facet of security required by an organization is linked to business objectives, and provides metrics to measure it. Case studies effectively demonstrate specific ways that metrics can be implemented across an enterprise to maximize business benefit. With three decades of enterprise information security experience, author Krag Brotby presents a workable approach to developing and managing cost-effective enterprise information security.

About the AuthorEnterprise Security Architect, Thousand Oaks, California,