EDPACS: The EDP Audit, Control, and Security Newsletter

Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/uedp20

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

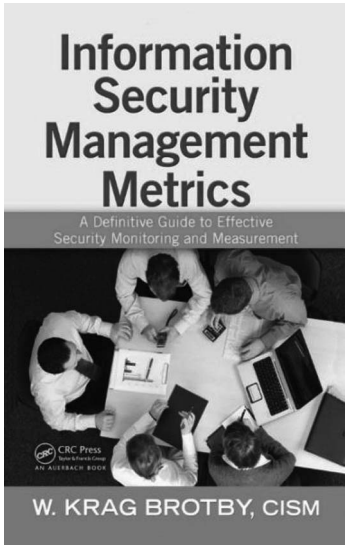
Gary Hinson

Published online: 30 Mar 2011.

To cite this article: Gary Hinson (2011) Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement, EDPACS: The EDP Audit, Control, and Security Newsletter, 43:3, 9-11

To link to this article: http://dx.doi.org/10.1080/07366981.2011.560057

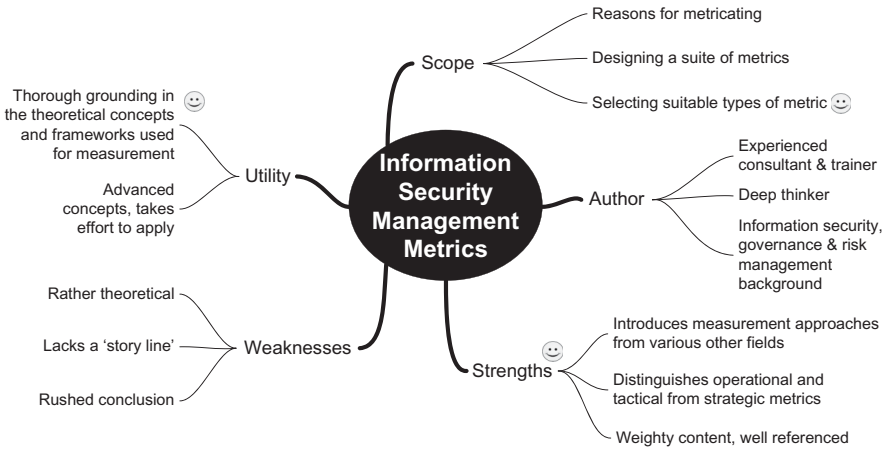
Book Review



INFORMATION SECURITY MANAGEMENT METRICS: A DEFINITIVE GUIDE TO EFFECTIVE SECURITY MONITORING AND MEASUREMENT

Author: Krag Brotby
ISBN: 978-1-4200-5285-5
Publisher: Auerbach/CRC Press (2009)
223 pages
Reviewed by Gary Hinson

SUMMARY



INTRODUCTION

Measuring 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 organization's Information Security Management System (ISMS). 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.

SCOPE OF THE BOOK

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.

The reasons for measuring information security are emphasized throughout the book. We are prompted to think of metrics specifically as a decision support tool, meaning that measurements which don't support meaningful management decisions are irrelevant. Parallels are drawn with the selection of instruments on an aircraft flight deck: there is literally no room for unnecessary or misleading dials and gauges. Describing different types of metrics helps us plan which metrics to include or exclude from our metrics system by applying a set of 8 criteria laid out succinctly in chapter 7 and taking into account their purposes described throughout the book.

ABOUT THE AUTHOR

Krag Brotby CISM CGEIT is a knowledgeable information security consultant with more than two decades' information security management experience in big-name companies. Krag has written and maintained the CISM review manual since 2005, and teaches workshop courses on CISM, governance, metrics and related topics.

THE BOOK'S STRENGTHS

Systematically managing practically anything requires meaningful metrics, so a look at management and measurement practices beyond the traditional bounds information security management is enlightening. Financial measures such as Return On Investment, for instance, are widely used to assess and compare the value of investments. The pros and cons of ROI methods such as Net Present Value and Internal Rate of Return are outlined, helping readers decide which methods might be appropriate for them. Introducing measures of organization structure and culture sets this security metrics book apart from most others.

Strategic, tactical and operational metrics are differentiated according to their predictive timescales and perspectives. The Information Security Manager may need to know, for example, exactly how many IT systems are up to date with the latest security patches in order to push the patching process along, but the CISO or CIO is probably happy to leave such details to the ISM, just so long as the residual risk from unpatched systems is broadly acceptable - which perhaps implies a need for assurance measures.

Although the writing style is clear, this is a complex subject covered in depth. The book is certainly thought-provoking. Roughly 50 books, papers and websites are cited for further study.

ITS WEAKNESSES

The book is rather theoretical or academic in approach. It won't suit practitioners simply looking for a short checklist of security things to measure, but takes considerable effort to comprehend and apply.

It is quite hard to make out the sequence or story-line to the book. Some parts are somewhat repetitive and might perhaps have been combined and rationalized (e.g. chapter 8 on information security governance and chapter 10 on information security governance metrics). A few are rather brief (e.g. chapter 14 on incident management and response outlines the kinds of questions that might be relevant but stops short of describing suitable metrics). The concluding chapter is particularly weak, as if the publication deadline cut it short.

There are few mathematical sections in the book but this is at once both a strength and a weakness. It is weak in the sense that the probabilistic nature of information security complicates trends analysis and prediction and so demands a reasonable understanding of statistics to generate meaningful numbers. On the other hand, there are many excellent books on statistics. Some additional references in this area might have been useful.

UTILITY OF THE BOOK

If you have the interest and time to study Information Security Management Metrics, you will be rewarded with a deeper and more rounded understanding of the issues involved in designing a system of metrics to help manage and improve information security. As such, the book is probably of most value to CISOs and ISMs tasked with implementing better security metrics in the context of an ISMS, and to information security management students.

CONCLUSION

Overall, I enjoyed studying this book and found the effort worthwhile but, being a pragmatist by nature, I was left wanting more in the way of practical guidance. At least with the theoretical background, I have the confidence to challenge commonplace but essentially useless metrics such as *Number of viruses detected in the past month*!

Dr. Gary Hinson, Ph.D., MBA, CISSP, is an information security specialist with a particular interest in the human aspects. Gary's career stretches back to the mid-1980s as a practitioner, manager and consultant in the fields of IT system administration, information security and IT auditing. Gary runs the information security awareness service NoticeBored and spends his days writing creative security awareness materials for subscribers. By night, Gary is a passionate supporter of the ISO/IEC 27000-series "ISO27k" information security management standards. Visit his website ISO27001security.com for ISO27k information, guidance and tools.