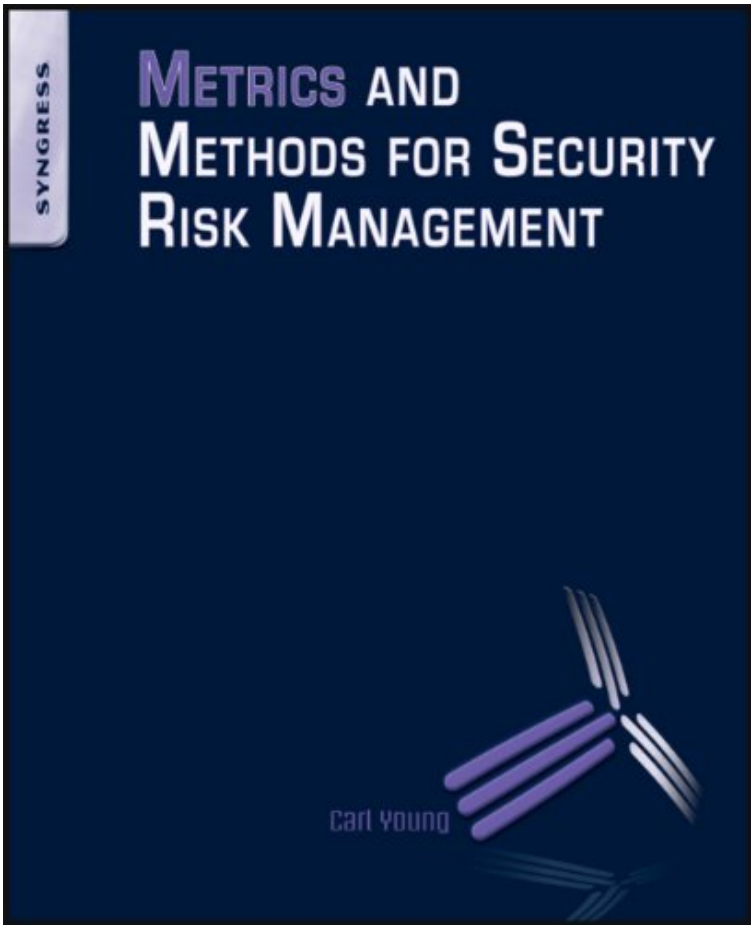
Metrics and Methods for Security Risk Management

Carl Young
*DOC | *audiobook | ebooks | Download PDF | ePub*



#1506441 in eBooks 2010-08-21 2010-08-21File Name: B004P1JFD8 | File size: 24.Mb

Carl Young : Metrics and Methods for Security Risk Management before purchasing it in order to gage whether or not it would be worth my time, and all praised Metrics and Methods for Security Risk Management:

0 of 1 people found the following review helpful. A Must Read For Security Professionals!By Thomas A. SkoulisSimply, the very best, most informative and educational reference for today's Security Professional. If you are responsible for developing a strategic security vision for your enterprise, this is a must read. This is a contemporary book that more than accurately frames today's security challenges with excellent analytic based assessment.1 of 1 people found the following review helpful. Good for IT, manufacturing and government security risk managementBy AcetoRisk management as applied to the many domains of security has not had an easy transition, despite the applicability of common tools. There has been a well intentioned impotence about it that has been rocked by many real losses, and left to the squeaky wheel, the fear monger and the ignorantly blissful. There is any number of well intentioned, modest, frugal and fiduciary-minded consultants lurking. Risk management as a component of security is useful, rather vital, because it adds a statistical framework that helps financial and operational planning. It also helps in compliance, public relations/marketing and as an audit worthy and legally bolstering demonstration of your prudence and due care.Mr. Young first goes back to basics, i.e., high school mathematics. Remember logarithms? We have an

efficient aid to revive all these topics: decibels, distribution, deviations, etc. Logs are a great way of dealing with scale, particularly these days. We loose connection with scale too easily, leaving us vulnerable. Although risk management has almost always been predominantly quantitative, as soon as you venture out of the old, well understood risk management domains into a space such as security, you are lost in the woods.His initial discussion of physical risk models is fundamental; they belong in any risk assessment where there is a physical presence of, say, executives, political leaders, or data processing , high value operations, and inventories. He talks about physical concentration as a threat, but it can just as well be treated as a vulnerability, so too with physical distance. The computing cloud in the virtual sky is a security option, but it must come within the domain of risk assessment, if only as a cost/benefit benchmark. Proper graphical representation is vital to understanding, particularly for your larger community to see your approach. Make use of his models.Performance measurement is nearly absent from security risk management. But as any desktop user who is beset by antivirus sclerosis will tell you (loudly) performance is what security must ensure, not hamper. One must ponder what kind of decisions we might ponder if we had no or misleading performance reporting.I have always had a chart for conducting my physical inspections, but Mr. Young has a good one that I will incorporate gratefully as an improvement. However, I cannot help but point out that, in his methods (he sometimes has several for any given security control point), he fails to include the donkey as a method for his perimeter control checkpoint. I have made great use of them in the interior of Brazil as they are nosey and do not mind cameras and microphones. If anything, they are encouraged. But helpfully, he does include offsite storage, including electronic media. Having done this work for years, I can tell you that you could use this book quickly in the field with no other training. I would prefer to walk through a couple with an old hand, but otherwise you should do acceptably well.Part 2 then is measuring and mitigating. Calculating probability (this might sound silly) in stats class is easier than doing it on the job, though the math is identical. I tend to uneconomic over protection, especially if I am not feeling confident about the underlying assessment in the first place. So I go back to Part 1; measure twice, cut once. Even so, having the presentation from the security risk management point of view is helpful. Little things like the Weibull variation on distribution theory targeted at reliability will not be mentioned in stats class. I had to look it up.Several more specialized areas are included: signal interception, explosives, radiation, chem and biohazard. I liked the one on network virus infections. So chances are you will not use every chapter. But there is not one disappointment here. Please vote "Yes" if you found this helpful. Thank you.1 of 1 people found the following review helpful. Who is its intended audience?By Kanishk RastogiBeing a Security Professional with a few years of experience, the title of the book appealed immediately as something different from what I'm used to reading. This book is not a typical Information Technology (IT) Security read, but, one that spans all forms of risk assessment, IT being one piece of it.The first few chapters are introductory and help the reader ease into what lies ahead.However, right after that, I had a hard time getting the authors point. I tried to read the book a few times with an intent to focus on cover-to-cover reading as I was expecting to learn something interesting and useful.However, that didn't happen. I even randomly picked up chapters going by the chapter titles, but saw the same problem. The author wants to cover a lot, so the book gets too generic several times and loose focus. It made me what audience it was intended to cater to. It seem to be too sophisticated for a casual read but not too specific either to qualify as a specialized reference.The concepts get repetitive several times. The author does come across as a knowledgeable person, but maybe couldn't decide what all to cover in one book. And that's where he faltered.The book would be better if some practical examples were provided, without which it become quite theoretical and hence keeps from keeping the reader engaged.P.S.: This review is written by my spouse who is a mobile security professional as my Vine obligation.

Security problems have evolved in the corporate world because of technological changes, such as using the Internet as a means of communication. With this, the creation, transmission, and storage of information may represent security problem. Metrics and Methods for Security Risk Management is of interest, especially since the 9/11 terror attacks, because it addresses the ways to manage risk security in the corporate world. The book aims to provide information about the fundamentals of security risks and the corresponding components, an analytical approach to risk assessments and mitigation, and quantitative methods to assess the risk components. In addition, it also discusses the physical models, principles, and quantitative methods needed to assess the risk components. The by-products of the methodology used include security standards, audits, risk metrics, and program frameworks. Security professionals, as well as scientists and engineers who are working on technical issues related to security problems will find this book relevant and useful. Offers an integrated approach to assessing security riskAddresses homeland security as well as IT and physical security issuesDescribes vital safeguards for ensuring true business continuity

nbsp;"Carl S. Young, VP [and senior risk strategist at a major international corporation], has delivered a volume to make the technology bedrock of security more comprehensible. To justify any security measure, Young shows how risk management can be understood quantitatively. That's important because so many workplace decisions on vulnerability are made after calculating risk metrics."--Security Letter, Vol. XL, No. 9 (September 2010) ".This author has a unique and useful perspective on an important and timely topic."-- Jon A. Schmidt, PE, BSCP, Director of

Antiterrorism Services, Burns McDonnell, Kansas City, MO. "Dealing with security risks requires not only the wisdom and experience to assess threats, but also the scientific and technical knowledge to mitigate their risk. Carl Young's wide-ranging expertise in both these areas has been recognized and honored during his distinguished career in government and in the private sector, and informs this fascinating book.[T]his book will be valuable to security professionals as well as concerned citizens."--Prof Emeritus Sidney Drell, Deputy Director,nbsp;Stanford Linear Accelerator Center (1969-1998). "In the post 9/11 world we had to find cost effective, practical, risk-based, resilient solutions to immensely challenging issues. Carl Young was, and is, central to that work. He combines academic brilliance with practical, hands-on experience of delivering security solutions. This book is a synthesis of that work."--James A. King, CBE, Senior UK government security and counterterrorism advisor (1978-2008). Head of Security and Fraud, Lloyds Banking Group, UK. "There is nobody in the field of security who surpasses Carl Young's experience and expertise. And now, for the benefit of us all, he has written Metrics and Methods for Security Risk Management. From the thoughtful layout of the chapters, to the clarity of his language and examples, Carl has given the gi...About the AuthorCarl S. Young is a recognized subject matter expert in information and physical security risk management. He is currently a Managing Director and the Chief Security Officer at Stroz Friedberg, an international security risk consulting firm. He is the former Global Head of Physical Security Technology at Goldman Sachs as well as a former Senior Executive and Supervisory Special Agent at the FBI. He was also a consultant to the JASON Defense Advisory Group. Mr. Young is the author of Metrics and Methods for Security Risk Management (Syngress, 2010), and The Science and Technology of Counterterrorism (Butterworth-Heinemann, 2014) as well as numerous journal publications. In 1997 he was awarded the Presidentrsquo;s Foreign Intelligence Advisory Board (PFIAB) James R. Killian Award by the White House for significant individual contributions to U.S. national security. Mr. Young received undergraduate and graduate degrees in mathematics and physics from the Massachusetts Institute of Technology.