Review of the book

"The Security Risk Assessment Handbook A Complete Guide for Performing Security Risk Assessments "

by Douglas J. Landoll
CRC Press, 2011

ISBN: 978-1-4398-2148-0

Yeşem Kurt Peker
TSYS School of Computer Science
Columbus State University

13 June 2013

1 Summary of the review

As its title promises, The Security Risk Assessment Handbook - A Complete Guide for Performing Security Risk Assessments provides a complete guide for undertaking a security risk assessment project and does a phenomenal job in doing that! The author draws on his years of experience to provide insight into various aspects of managing an assessment project in general, and a security assessment project in particular. He divides a security risk assessment project into various phases including Project Definition, Project Preparation, Data Gathering, Risk Analysis, Risk Mitigation, and Risk Reporting and Resolution and discusses each phase in detail. Whenever appropriate he provides tables, charts, and sample reports from real-life cases which would be very hard to find elsewhere.

The book is an invaluable resource for anyone who plans to step into the profession of security risk assessment. It covers almost all practical matters in security risk assessment in great detail from the manners in interacting with the customer to technical aspects. Where it is not possible to provide details (such as the details in mathematical analysis of the findings), it refers one to the relevant resources.

2 Summary of the book

The book is organized into 13 chapters. The first introductory chapter starts by discussing possible motivations behind a security initiative from the perspective of a security service consumer. It goes on to give a precise definition of a security risk assessment and discusses the need for a security risk assessment from a more general perspective. Some of the terminology used in the subsequent chapters are also introduced here.

The second chapter discusses the basic steps in security risk assessment and prepares the framework for the subsequent chapters. It divides the security risk assessment into 6 phases and briefly discusses what each phase is about. The six phases are called Project Definition, Project Preparation, Data Gathering, Risk Analysis, Risk Mitigation, and Risk Reporting and Resolution.

Chapter 3 discusses the significance of defining the project in terms of objectives, scope, budget, system boundaries, deliverables, level of rigor of analysis, and contract type. It emphasizes the importance of having the the customer on board and in agreement from the beginning of the project.

Chapter 4 is about preparations before the assessment starts on site at the customer location. These preparations include introducing the team to the organization, obtaining necessary permissions and accounts for testing and data gathering, and reviewing available information. They aid the assessment team in identifying the critical systems, assets, and threats. The chapter also discusses different approaches to determining asset criticality and valuation.

Chapter 5 is about data gathering. It discusses two common approaches in data gathering, namely sampling and RIIOT (Review, Interview, Inspect, Observe, and Test). Chapter 6,7,8 focus on administrative, technical, and physical data gathering respectively and provide the reader with an overview of the threats and safeguards relevant to each of these areas.

Chapter 9 discusses how all the information gathered in the previous phases are put together and analyzed to determine the security risks and create security risk statements.

Chapter 10 is about Risk Mitigation which refers to the process of developing safeguards and countermeasures to reduce the risks determined in the risk analysis phase. It discusses the selection of safeguards, compiling of safeguard solution sets, justifying the implementations of the safeguards and the essence of understanding the security risk parameters

Chapter 11 is on the reporting of the results of the assessment. It starts by stressing the importance of providing reports at various stages during the assessment process and provides guidelines on how to structure and tone a report so that it has the desired effectiveness on the customer.

Chapter 12 is about successful management of a security risk assessment project. It discusses project planning, tracking, correction and reporting. Most of the discussions would apply not only to a security risk assessment project but to any project in general. One part that is unique to security risk assessment is the part where descriptions of various certification standards in information security are provided.

Chapter 13 discusses quantitative and qualitative approaches in analyzing security risks. Strengths and weaknesses of both types of analyses along with examples of how they can be applied are provided. The chapter, although briefly, also talks about using established security risk assessment processes such as FAA, OCTAVE, FRAP, CRAPP, NSA IAM.

3 What is the book like (style)?

While providing complete guidelines for performing a security assessment project, the author emphasizes the uniqueness of each such project. He draws on his years of experience in industry and security risk assessment and shares with the reader valuable insight, tips and tools to conduct a successful security risk assessment project. Not only guidelines but also the reasonings behind them are provided as part of the discussions. In fact, much of the discussions in the book could apply to any kind of assessment project.

The author goes into great detail in all aspects of risk assessment particularly in data gathering. Data gathering is the most time consuming and a critical phase in an assessment. It is divided into three categories in security risk assessment depending on the source of the data. The three categories are administrative, technical and physical and each of them is discussed in a separate chapter in the book.

While reading the book the reader also gets familiar with different industries and the security standards that apply to them.

Each chapter in the book comes with a set of exercises for the reader to test his/her knowledge, do further thinking or do some research.

4 Would you recommend this book?

I would recommend the book to anyone who plans to step into the profession of security risk assessment as well as to people already in the business. It provides detailed insight into the the process of risk assessment and shares tips and lessons from experience one would not easily find anywhere else.

The security service consumer who wants to have a more in depth understanding of the security risk assessment will also benefit from reading this book; it will help them to more confidently scope their security risk analysis to meet their objectives.

The reviewer is an assistant professor at the TSYS School of Computer Science at Columbus State University in Columbus, GA.