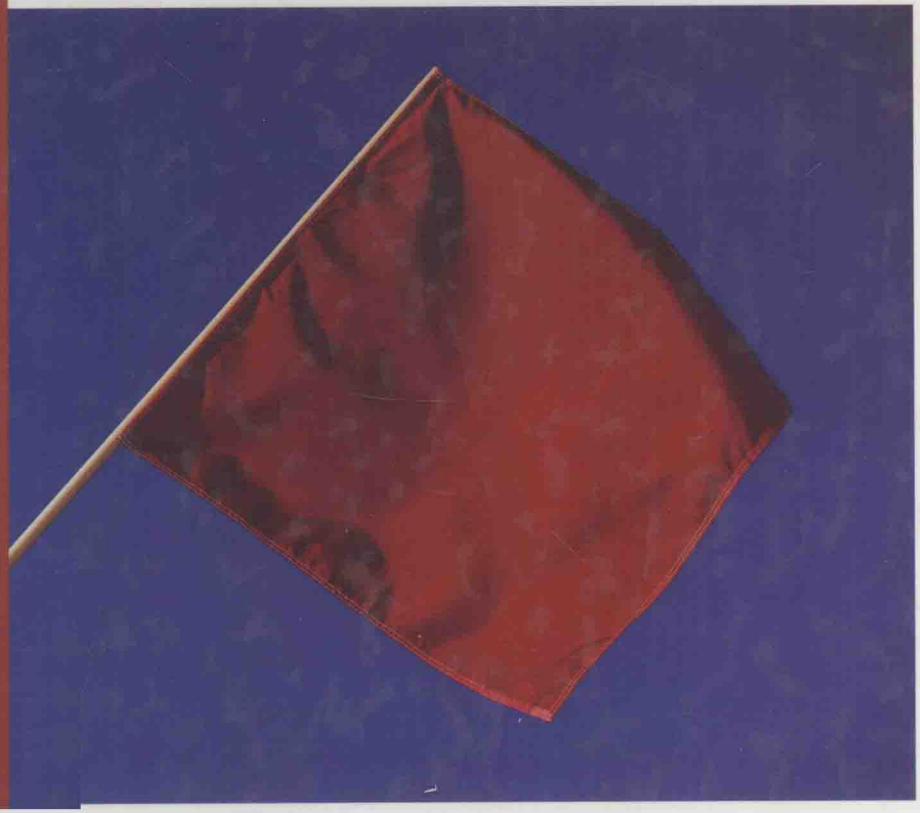
RISKS, CONTROLS, AND SECURITY

Concepts and Applications



VASANT RAVAL / ASHOK FICHADIA

1ST EDITION

RISKS, CONTROLS, AND SECURITY

Concepts and Applications

VASANT RAVAL
Creighton University

ASHOK FICHADIA
Union Pacific Corporation

BICENTENNIAL 1807 WILEY 2007 BICENTENNIAL

Publisher *Don Fowley*
Executive Editor *Christopher DeJohn*
Acquisitions Editor *Mark Bonadeo*
Senior Production Editor *Valerie A. Vargas*
Marketing Manager *Clay Stone*
Creative Director *Harry Nolan*
Senior Designer *Madelyn Lesure*
Production Management Services *Techbooks*
Editorial Assistant *Karolina Zarychta*
Media editor *Allison Morris*
Cover Photo *Corbis Digital Stock*

This book was set in 10/12 Times Roman by Techbooks and printed and bound by Malloy Incorporated. The cover was printed by Phoenix Color.

The book is printed on acid-free paper. ∞

ISBN-13 978-0-471-48579-7
ISBN-10 0-471-48579-7

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

RISKS, CONTROLS, AND SECURITY

Concepts and Applications

THE WILEY BICENTENNIAL–KNOWLEDGE FOR GENERATIONS

Each generation has its unique needs and aspirations. When Charles Wiley first opened his small printing shop in lower Manhattan in 1807, it was a generation of boundless potential searching for an identity. And we were there, helping to define a new American literary tradition. Over half a century later, in the midst of the Second Industrial Revolution, it was a generation focused on building the future. Once again, we were there, supplying the critical scientific, technical, and engineering knowledge that helped frame the world. Throughout the 20th Century, and into the new millennium, nations began to reach out beyond their own borders and a new international community was born. Wiley was there, expanding its operations around the world to enable a global exchange of ideas, opinions, and know-how.

For 200 years, Wiley has been an integral part of each generation's journey, enabling the flow of information and understanding necessary to meet their needs and fulfill their aspirations. Today, bold new technologies are changing the way we live and learn. Wiley will be there, providing you the must-have knowledge you need to imagine new worlds, new possibilities, and new opportunities.

Generations come and go, but you can always count on Wiley to provide you the knowledge you need, when and where you need it!

William J. Pesce

WILLIAM J. PESCE
PRESIDENT AND CHIEF EXECUTIVE OFFICER

Peter Booth Wiley

PETER BOOTH WILEY
CHAIRMAN OF THE BOARD

To Prafulla and Foram

Preface

Business environments, especially in the last ten years, have changed radically and will continue to change. Broadly, two factors responsible for this are information technology and globalization. With the introduction of the World Wide Web, existing businesses have changed, and new business models have emerged. The forces of technology cannot be ignored, but rather should be leveraged to keep business viable and growing. In part, the globalization of businesses is occurring due to the technology that provides a virtual environment, making physical constraints and political boundaries less significant.

With the changing environment, additional risks have appeared, whereas existing risks have changed in significance. This change is nonlinear; therefore, risks that surface from it don't fit the traditional mold. Although the tenets of security and control still remain nearly the same, its "how-to" dimension has undergone radical changes. Most new methods and revisions in existing methods of control and security have followed "out-of-the box" ideas and concepts. Although the objectives are the same, the behavior of people and systems is cast in a different situation. Protection of information assets in today's business world has gained much greater significance. Hardly a day passes without news of attacks on information assets, including identity theft, denial of service, and violation of privacy and confidentiality. Assurance of information security is therefore a key concern for designers, users, and evaluators of information systems. A whole new terminology has appeared on the scene whereas some of the age-old concepts, such as cryptography and trust, have taken greater significance in the digital economy.

The overall goal of this textbook is to provide a comprehensive understanding of information security issues, such as risks, controls, and assurance for information systems in a digital economy. We present in this book relevant concepts and their applicability in risk management. Current in its content and technically accurate, this book is accessible to those who have a limited understanding of computer-based systems and yet have a desire to comprehend requirements of and tools for information security.

A strong motivation behind writing this book is to help those interested in the field to gain a basic understanding of the new landscape of risks, controls, and security. In writing the book, we assume very little about the reader's background, except an interest in learning the topic and a basic understanding of computer-based systems. Where deemed necessary, we have included a primer on relevant technology to help you recall or learn pertinent concepts prior to delving into security issues. Thus, the book can help almost any student, professional, or manager gain an understanding and appreciation of the field.

ROLE IN LEARNING AND TEACHING

This book is designed to serve many roles. It can be used as a textbook in undergraduate curricula at about a junior or senior level at colleges and universities. Ideally, a second course in information systems, auditing, or accounting information systems will be served well by this book. An early course in graduate business or computer science programs can

also profit from the book. Outside the arena of higher education, professional training and certification programs can benefit from the book.

Although sticking to the fundamentals, the book is not written exclusively for a "survey" course, in that it covers the practice of concepts and models discussed. The book encourages not only the comprehension of key concepts, but also their applications.

▶ KEY FEATURES

In this book, we integrate learning material through a generous use of concept maps. A concept map is a knowledge representation tool. Essentially, concepts represent perceived regularities in events or objects, designated by a label. The concept mapping methodology is developed using Ausubel's theory of meaningful learning, which suggests that meaningful learning is a process in which new information is related to an existing relevant aspect of an individual's knowledge structure.

The use of concept maps in this book will facilitate systematic transition throughout the book. Concepts, such as risk factors and security principles, learned in early chapters are linked to the discussion in later chapters, providing a clear integration of topics. Although a message can easily get lost in verbal discussions, visuals can illustrate how the concepts discussed relate and come together. As an individual progresses through the chapters in the book, a clear understanding of relationships among concepts emerges, and partly because of that, a holistic understanding of the security domain is likely to occur.

We believe that the use of concept maps in this book has made it a much better learning resource. After studying a chapter, the reader can go to the concept maps and review if the map captures his or her understanding of the material. This kind of feedback can also provide guidance on which parts of the chapter the student should revisit for a better grasp of the subject matter.

To the extent possible, we have put to use concept maps in this book in a hierarchical form. Whereas a high-level map provides the beginning of a chapter, parts of the same map can later provide clues about the "local" area. Thus, this approach keeps the student from losing sight of the entire landscape!

In addition to concept maps, we have drawn analogies throughout the book to help the reader compare popular or known situations with information security scenarios. We hope such comparisons will lead to meaningful learning of risk, control, and security concepts. It is important to note, however, that analogies may be limited or incomplete and should be drawn with caution.

Finally, every chapter in the book begins with a Security in Practice case relevant to the chapter content. We have included additional Security in Practice cases, where appropriate in the chapters, and also in end of chapter exercises. We believe these cases (1) have recent origins, (2) are relevant to the learning objective(s) and (3) raise or address issues that are fundamental in the subject area.

This book is distinguished by:

- Clear and accurate in communication of rather difficult and new concepts
- Integration of topics through the use of concept maps and submaps throughout the book
- Real-world and current applications of concepts discussed in the book

- Solid and accurate technical content balanced against related managerial content, delivered in a manner that facilitates learning.
- Discussion of issues as they apply to *all* businesses, not just e-business
- Content covers both theoretical and practical dimensions of topics. This has become possible due to the team of coauthors, one from higher education and the other from business.

ORGANIZATION AND CONTENT

This book is about risk management of information systems in today's information systems environment. The first three chapters provide the foundation for the remaining book. Chapter 1 covers a discussion of enterprise and its risks, and concludes with the relationship between organization and its information systems, especially as concerns risks. Chapter 2 is devoted to principles and practices that provide the foundation for risk management, with specific reference to information systems risks. Moreover, basic concepts in information security solutions are also covered here. Chapter 3 builds on the first two chapters by articulating control and risk management frameworks and their role in information security.

Included among the control and security frameworks is the COSO framework. The importance of the framework has greatly increased since the passage of the Sarbanes-Oxley Act of 2002. To cover additional material related to the new regulatory requirement, two appendixes have been added to the Chapter 3. Appendix 3.1 briefly summarizes Section 404 of the Act; its discussion signals the importance of implementing a control framework. Appendix 3.2 illustrates the process of implementing controls using a case study.

Business continuity and systems availability are the topics of Chapter 4. Most concepts here address the management side of the issues; hence the chapter's placement just prior to the beginning of predominantly technical areas is appropriate. Only one other chapter, Chapter 13, can be considered mostly nontechnical in coverage; however, a basic understanding of technical aspects of information security is a prerequisite for this chapter, particularly the section on regulation.

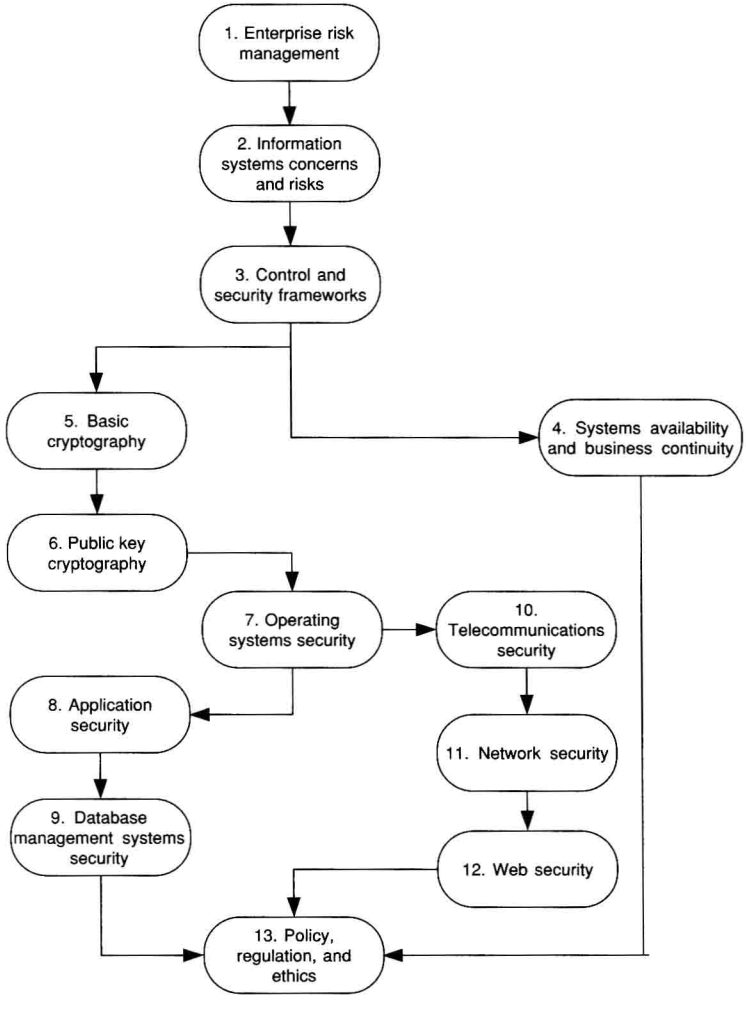
Because encryption is central to many of the information security solutions, concepts and applications of encryption technologies are included in two chapters. Chapter 5 begins with the notion of encryption and covers both secret key and public key encryption. Chapter 6 is devoted primarily to applications of public key encryption, particularly in the form of public key infrastructure.

The next six chapters can be logically divided into two groups: somewhat familiar domains and relatively new domains of security. Three chapters (Chapters 7, 8, and 9) cover the former, and the next three (Chapters 10, 11, and 12), the latter. Included among the familiar domains are operating systems security, database management systems security, and application security. Inasmuch as these themes are called "familiar" here, we should keep in mind that they, too, have changed considerably with the presence of the Internet. We cover not only their traditional, but also their current roles in relation to information security. Relatively new areas of information security emerge essentially from the presence of the Web and the resulting netcentric world. Telecommunications provide the synergies and challenges of the networked systems. In form, networked systems have grown beyond local areas and present new challenges in risk management. Using the Web, such networks

are extended beyond the boundaries of an entity, and this brings new opportunities and risks. Chapter 10 is devoted to telecommunications security, Chapter 11 to network security, and Chapter 12 to Web security.

As noted previously, the final chapter (Chapter 13) returns to the administrative side of information security. Under the umbrella of security administration, topics discussed here are security policy development, compliance with regulations, and nurturing ethical behavior within an organization. Because social engineering is close to all these issues, its discussion is also included in the chapter.

Although there are several ways in which these topics can be covered, one particular sequence is shown in the following concept map.



Concept map A sequence of chapter coverage

SUPPLEMENTS ACCOMPANYING THE TEXT

Solutions Manual

The Solutions Manual, by the text authors, contains responses to the end-of-chapter discussion questions and exercises. Answers to the end-of-chapter multiple-choice items are included in the book at the end of exercises for the chapter. These items provide students a source of learning concepts and their applications.

Lectures in PowerPoint

As a supplement, PowerPoint slides are available to instructors for use in preparing and displaying material for lectures.

Product Support Web Site

To assist instructors and students, a product support Web site has been created at the publisher's site. This Web site will complement the book and facilitate and enhance learning. For additional resources and current developments in the field of information security, please access the site.

A glossary of terms is provided as a single source of reference to trace the key concepts throughout the book.

Acknowledgments

We wish to acknowledge the helpful suggestions provided by the following reviewers:

Amelia A. Baldwin
University of Alabama, Tuscaloosa

Somnath Bhattacharya
Florida Atlantic University

Thomas G. Calderon
University of Akron

Lei-da Chen
Creighton University

Greg Freix
University of Kansas

Jagdish S. Gangolly
SUNY, Albany

Gary W. Hansen
Brigham Young University

Stacy E. Kovar
Kansas State University

Vincent E. Owhosa
Bentley College

Sujeet Shenoi
University of Tulsa

Karem Tomak
University of Texas, Austin

L. Melissa Walters
Loyola University, New Orleans

Alfred Zimmerman
University of Hawaii

We have been fortunate in the ample support provided by key individuals at John Wiley: Mark Bonadeo, who guided us throughout the book development; Valerie A. Vargas, who moved us smoothly through the production stage; and Ervin E. Smith, who encouraged us to develop and pursue this project. We gratefully acknowledge excellent support from the entire Wiley team. Karen A. Slaght provided excellent assistance in editing the manuscript and Dennis Free, in getting the copy ready for production.

We are grateful to many people for their assistance in this significant project. Kristine Protzman and Kelly Kruse offered dedicated support in the initial editing and organization of the text. Their continuous feedback and valuable suggestions have helped improve the organization of the book and the communication of its content. Kyle Haynes and Justin Snyder contributed greatly in research on technical topics. Abrams O'Bayounge provided excellent support in literature search and later in the development of PowerPoint lectures and the solutions manual. Chandni Sarawagi and Rucha Raval reviewed much of the text material and also helped with the solutions manual. In addition, a number of students over the past two years participated in testing the textbook material and end-of-chapter questions and exercises. With their help the text has become a meaningful learning resource for future students and professionals.

We sincerely hope that this book will provide you just the kind of support that you need in learning about and teaching information security concepts. We welcome your comments and suggestions.

Vasant Raval
Ashok Fichadia

About the Authors

VASANT RAVAL

Vasant Raval currently serves as Professor of Accounting at Creighton University. He received his Doctor of Business Administration degree from Indiana University in 1976. Prior to joining Creighton University in 1981, he was a faculty member at the University of Windsor, Ontario, Canada. He has also worked as a management accountant and auditor in industry and government in India. His expertise includes information security, information technology management, accounting information systems, management control systems, and corporate governance. He holds professional certifications in information systems audit and control and in management accounting.

An active member of the Information Systems Audit & Control Association, Vasant has several articles published in journals including *The Journal of Information Systems, Management Accountant (India), IS Audit & Control Journal, Information Strategy: The Executive's Journal, The Technological Horizons in Education Journal,* and *Information and Management.* His monograph, "Videotex in Education: An Empirical Study," received international exposure. He has previously served on the Editorial Review Boards of *The Journal of Information Systems, IS Audit & Control Journal* and *Auditing: A Journal of Practice and Theory,* and has worked as an ad hoc reviewer for *Decision Sciences, Accounting Horizons,* and *Issues in Accounting Education.* He is a co-author of the fourth edition of *Accounting Information Systems: Essential Concepts and Applications* (Wiley, 2000).

Vasant is a member of several professional organizations and cultural associations. During 2001–02, he was President of AIS Educators Association, a national network of accounting educators interested in teaching and research in AIS. He teaches financial and managerial accounting, accounting information systems, and digital security at Creighton University, where he served as Associate Dean and Director of Graduate Business Programs (1987–96) and as Chair of the Department of Accounting (2001–06). Currently, he is a member of the Douglas County audit committee, serves on the board of directors at InfoUSA, Inc. and Syntel, Inc. and chairs the audit committee of each company's board.

ASHOK FICHADIA

Ashok Fichadia is the president and chief executive officer of PS Technology, a wholly-owned subsidiary of Union Pacific Corporation. In his current role, Ashok is responsible for strategic direction of the Company and the delivery of value-added software products to solve real business problems within the transportation industry. Prior to this appointment, Ashok was Director of Systems Engineering within the Information Technology department of Union Pacific Railroad where he led the implementation of speech and telephony technology to automate transactions via self-service solutions.

Ashok managed the information security audit group within Union Pacific Corporation for several years. As part of this tenure, Ashok gained hands-on experience and knowledge of the risks, controls, and mitigation techniques related to enterprise security. He led several tiger-team attacks on the company's information technology infrastructure to uncover weaknesses and provided recommendations to mitigate them. In addition, he built several tools and scripts to automate security assessment of various environments. He has taught classes on information security auditing to audit professionals at the Institute of Internal Auditors, and has developed and delivered a graduate-level class on the subject at the University of Kansas.

Ashok holds a bachelor's degree in engineering from Indian Institute of Technology, Mumbai, India, and master's degrees in engineering and business administration from the University of Kansas. He is CISA-certified and currently serves on the technical advisory board of Onstate Communications.

Brief Contents

Contents