INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES

ISSA

Fundamentals of Information Systems Security

FOURTH EDITION

David Kim | Michael G. Solomon

JONES & BARTLETT
LEARNING

World Headquarters
Jones & Bartlett Learning
25 Mall Road
Burlington, MA 01803
978-443-5000
info@jblearning.com
www.jblearning.com

Jones & Bartlett Learning books and products are available through most bookstores and online booksellers. To contact Jones & Bartlett Learning directly, call 800-832-0034, fax 978-443-8000, or visit our website, www.jblearning.com.

Substantial discounts on bulk quantities of Jones & Bartlett Learning publications are available to corporations, professional associations, and other qualified organizations. For details and specific discount information, contact the special sales department at Jones & Bartlett Learning via the above contact information or send an email to specialsales@jblearning.com.

24458-8

Production Credits

Vice President, Product Management: Marisa R. Urbano
Vice President, Product Operations: Christine Emerton
Director, Content Management: Donna Gridley
Director, Project Management and Content Services: Karen Scott
Product Manager: Ned Hinman
Content Strategist: Melissa Duffy
Content Coordinator: Mark Restuccia
Development Editor: Kim Lindros
Technical Editor: Jeffrey Parker
Project Manager: Jessica deMartin
Senior Project Specialist: Jennifer Risden
Digital Project Specialist: Rachel DiMaggio
Marketing Manager: Suzy Balk
Product Fulfillment Manager: Wendy Kilborn
Composition: Straive
Cover Design: Briana Yates
Media Development Editor: Faith Brosnan
Rights Specialist: Benjamin Roy
Cover Image (Title Page, Front Matter Opener, Part Opener, Chapter Opener): © Ornithopter/Shutterstock
Printing and Binding: McNaughton & Gunn

Library of Congress Cataloging-in-Publication Data

Names: Kim, David (Information technology security consultant) | Solomon, Michael (Michael G.), 1963– author.
Title: Fundamentals of information systems security / David Kim, Michael G. Solomon.
Description: Fourth edition. | Burlington, Massachusetts : Jones & Bartlett Learning, [2023] | Includes bibliographical references and index.
Identifiers: LCCN 2021021301 | ISBN 9781284220735 (paperback)
Subjects: LCSH: Computer security. | Computer networks—Security measures. | Information storage and retrieval systems—Security measures.
Classification: LCC QA76.9.A25 K536 2023 | DDC 005.8—dc23
LC record available at https://protect-us.mimecast.com/s/jX-ACERyDytkrO95Spo_zS?domain=lccn.loc.gov

6048

Printed in the United States of America

25 24 23 22 21 10 9 8 7 6 5 4 3 2 1

This book is dedicated to our readers and students and the IT professionals pursuing a career in information systems security. May your passion for learning IT security help you protect the information assets of the United States of America, our businesses, and the private data of our citizens.
—David Kim

To God, who has richly blessed me in so many ways.
—Michael G. Solomon

Contents

Preface

Purpose of This Text

This text is part of the Information Systems Security & Assurance (ISSA) Series from Jones & Bartlett Learning (*www.issaseries.com*). Designed for courses and curriculums in IT Security, Cybersecurity, Information Assurance, and Information Systems Security, this series features a comprehensive, consistent treatment of the most current thinking and trends in this critical subject area. These titles deliver fundamental information security principles packed with real-world applications and examples. Authored by Certified Information Systems Security Professionals (CISSPs) and experienced cybersecurity consultants, this series delivers comprehensive information on all aspects of information security. Reviewed word for word by leading technical experts in the field, these texts are not just current but forward thinking—putting you in the position to solve the cybersecurity challenges not just of today but also of tomorrow.

Part I of this text on information security fundamentals focuses on new risks, threats, and vulnerabilities associated with the transformation to a digital world and the Internet of Things (IoT). Individuals, students, educators, businesses, organizations, and governments have changed how they communicate, share personal information and media, and do business. Led by the vision of the IoT, the Internet and broadband communications have entered into our everyday lives. This digital revolution has created a need for information systems security. With recent compliance laws requiring organizations to protect and secure private data and reduce liability, information systems security has never been more recognized than it is now.

Part II is adapted from CompTIA's Security+ professional certification. CompTIA's Security+ is the most widely accepted foundational, vendor-neutral IT security knowledge and skills professional certification. As a benchmark for foundational knowledge and best practices in IT security, the Security+ professional certification includes the essential principles for network security, operational security, and compliance. Also covering application, data, and host security, threats and vulnerabilities, access control, identity management, and cryptography, the Security+ certification provides a solid foundation for an IT security career.

Part III of this text provides a resource for readers and students desiring more information on information security standards, education, professional certifications, and recent compliance laws. These resources are ideal for students and individuals desiring additional information about educational and career opportunities in information systems security.

New to This Edition

This new edition has been updated to reflect the security environments you will encounter in today's organizations. The content has been slightly reorganized, extended, and refreshed to ensure that it covers the latest trends, standards, and industry best practices. Part I, The Need for Information Security, covers how today's complex business environments have changed due to technological and cultural influences and how those changes impact security. Part II, Securing Today's Information Systems, continues the discussion from Part I to form the core material of the text. In Part II we dig into the various aspects and domains of cybersecurity and discuss how security applies in each case. This edition retains the technical information from previous editions but frames discussions in the context of satisfying business goals at the strategic level. Additional focus is placed on continuity and emerging strategic concerns. And, finally, Part III, Information Security Standards, Certifications, and Laws, presents an up-to-date overview of various external governance influences that inform security-related decisions and strategy. This latest edition provides the most comprehensive coverage to date of how to implement enterprise security as a strategic organizational objective.

Cloud Labs

This text is accompanied by Cybersecurity Cloud Labs. These hands-on virtual labs provide immersive mock IT infrastructures where students can learn and practice foundational cybersecurity skills as an extension of the lessons in this text. For more information or to purchase the labs, visit *go.jblearning.com/Kim4e*.

Learning Features

The writing style of this text is practical and conversational. Step-by-step examples of information security concepts and procedures are presented throughout the text. Each chapter begins with a statement of learning objectives. Illustrations are used to clarify the material and vary the presentation. The text is sprinkled with Notes, Tips, FYIs, Warnings, and Sidebars to alert the reader to additional helpful information related to the subject under discussion. Chapter assessments appear at the end of each chapter, with solutions provided in the back of the text.

Chapter summaries are included in the text to provide a rapid review or preview of the material and to help students understand the relative importance of the concepts presented.

Audience

The material is suitable for undergraduate or graduate computer science majors or information science majors, students at a two-year technical college or community college who have a basic technical background, or readers who have a basic understanding of IT security and want to expand their knowledge.

Acknowledgments

I would like to thank Michael Solomon, for taking the lead authoring role on this fourth edition, and to the Jones & Bartlett Learning team led by Ned Hinman. This journey that we have been on together from the first to the fourth edition has allowed us to significantly impact the lives of new cybersecurity professionals across the country as well as protect our information assets.

This fourth edition book project commenced during the COVID-19 pandemic, which prevented me from being able to physically visit and spend quality time with my mom, Mrs. Yum Kim.

I would like to thank my mom for her unconditional love and for guiding me into the man I have become.

David Kim

I would like to thank David Kim and the whole Jones & Bartlett Learning team for providing pertinent editorial comments and for helping to fine-tune the book's content. All of you made the process so much easier and added a tremendous amount of value to the book. I want to thank God for blessing me so richly with such a wonderful family, and for my family's support throughout the years. My best friend and wife of over three decades, Stacey, is my biggest cheerleader and supporter through many professional and academic endeavors. I would not be who I am without her.

Both of our sons have always been sources of support and inspiration. To Noah, who still challenges me, keeps me sharp, and tries to keep me relevant, and Isaac, who left us far too early. We miss you, son.

Michael G. Solomon

The Authors

David Kim is the president of Security Evolutions, Inc. (SEI; *www.security-evolutions.com*), located outside the Washington, DC, metropolitan area. SEI provides governance, risk, and compliance consulting services for public and private sector clients globally. SEI's clients include health care institutions, banking institutions, governments, and international airports. SEI's IT security consulting services include security risk assessments, vulnerability assessments, compliance audits, and designing of layered security solutions for enterprises. In addition, available services include developing business continuity and disaster recovery plans. Mr. Kim's IT and IT security experience encompasses more than 30+ years of technical engineering, technical management, and sales and marketing management. This experience includes LAN/WAN; internetworking; enterprise network management; and IT security for voice, video, and data networking infrastructures. He is an accomplished author and part-time adjunct professor who enjoys teaching cybersecurity to students across the United States.

Michael G. Solomon, PhD, CISSP, PMP, CISM, CySA+, Pentest+, is an author, educator, and consultant focusing on privacy, security, blockchain, and identity management. As an IT professional and consultant since 1987, Dr. Solomon has led project teams for many Fortune 500 companies and has authored and contributed to more than 25 books and numerous training courses. Dr. Solomon is a professor of cyber security at the University of the Cumberlands and holds a PhD in computer science and informatics from Emory University.