Information Security

FOR MANAGERS

Michael Workman, PhD
Professor, Nathan M. Bisk College of Business
Director, Security Policy Institute
Florida Institute of Technology

Daniel C. Phelps, PhD
Assistant Teaching Professor
Information Systems Program
Carnegie Mellon University in Qatar

John N. Gathegi, PhD, JD
Professor, School of Information
Courtesy Professor, School of Mass Communications
University of South Florida

JONES & BARTLETT
LEARNING

World Headquarters
Jones & Bartlett Learning
5 Wall Street
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.

Copyright © 2013 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

All rights reserved. No part of the material protected by this copyright may be reproduced or utilized in any form, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the copyright owner.

Production Credits:
Publisher: Cathleen Sether
Senior Acquisitions Editor: Timothy Anderson
Senior Associate Editor: Amy Bloom
Director of Production: Amy Rose
Production Assistant: Alyssa Lawrence
Senior Marketing Manager: Andrea DeFronzo
V.P., Manufacturing and Inventory Control: Therese Connell
Composition: Laserwords Private Limited, Chennai, India
Cover Design: Scott Moden
Rights and Permissions Manager: Katherine Crighton
Rights and Photo Research Supervisor: Anna Genoese
Cover Image: © Sean Gladwell/ShutterStock, Inc.
Printing and Binding: Malloy, Inc.
Cover Printing: Malloy, Inc.

Library of Congress Cataloging-in-Publication Data
Workman, Michael D., 1957-
Information security for managers / Michael Workman, Daniel C. Phelps, and John N. Gathegi.
p. cm.
Includes index.
ISBN-13: 978-0-7637-9301-2 (pbk.)
ISBN-10: 0-7637-9301-9 (pbk.)
1. Information technology—Security measures. 2. Computer security—Management. 3. Computer networks—Security measures. 4. Business enterprises—Security measures. I. Phelps, Daniel C. II. Gathegi, John Ng'ang'a. III. Title.
HF5548.37.W67 2013
658.4'78—dc23

2011033490

6048
Printed in the United States of America
16 15 14 13 12 10 9 8 7 6 5 4 3 2 1

Contents

SECTION TWO Technology Orientation for Managers 121

Preface

Welcome to *Information Security for Managers*! This textbook will provide you with an overview of conceptual and applied knowledge of information and systems security and will offer a summary overview of security concepts that are addressed in more technical detail in Jones & Bartlett Learning's Information Systems Security & Assurance series. Our goal is to provide a reference textbook suitable for computer science and information technology students in the area of what is known as "*knowledge work,*" and to introduce the concepts you may read in the series if you seek more in-depth technical knowledge. The text is also suitable for managers desiring to learn more about information security. This textbook is divided into four sections dealing with major aspects of security in which the reader needs to be familiarized: policies and procedures, technology orientation, computer and network security, and managing organizations securely. We present most of the material at a conceptual level, but, where we believe appropriate, we also delve into some of the more technical details to give the audience insights into critical security issues at the "implementation" level.

Why Study Information Security?

Security is important to managers because although information systems have improved over the years to become more effective in collecting and rendering information for human consumers, these improvements have been accompanied by increases in the frequency and sophistication of attacks against them. The impacts from attacks against companies are significant, and managers are responsible for their organizations, including security. Failures can cause significant losses to companies and to their suppliers and clients, may cost managers their jobs, and can even lead to legal liabilities that are adjudicated against them.

Unintentional and Intentional Security Failures

Examples of where the consequences of information security failures can come into play include hospital emergency rooms, rail transportation control rooms, and power grids. In hospital emergency rooms, physicians use technology to evaluate the relationships among indicators of illnesses when they review signs and symptoms, laboratory information, and results of specialized diagnostic studies or cases in order to diagnose acute patient conditions and decide on treatments. If compromised, this information could lead to severe consequences. There is a growing threat that an employee at a hospital or clinic might steal patient information and sell it on the black market for the purposes of identity theft and insurance fraud. In rail transportation control rooms, trains are electronically dispatched and switched between myriad tracks according to situational variables such as train and crew operability, and containers' contents and schedules. Compromised information can lead to catastrophes, as seen when two Burlington Northern Santa Fe (BNSF) railroad trains collided in 2010. In power grids, there are tens of thousands of different kinds of generators that must be electronically managed and monitored for electrical power output, temperature, power redirection, and unit failures, which could be compromised by attackers or disrupted simply as a cause of human or machine error.

Technologies, Time Zones, and Geography

Technologies are rapidly advancing in their capabilities, but along with these advancements come new security problems. For instance, widely available spyware software that targets mobile phones can remotely activate the phone and be used by third parties to track a person's whereabouts, read text messages from the phone, and even listen in on phone conversations. Surface computing, grid computing, cloud computing, and semantic technologies and software agents are all emerging (often called "disruptive") technologies that are being implemented well ahead of adequate security measures that might protect them. We now have to think about Software as a Service (SaaS), and we will soon have to contend with intelligent bots, called "agents," that may not only "visit" our computers to gather information and carry out instructions, but also execute instructions that are given to them, such as to make reservations through an airline or restaurant web page. Now we will have to think about the security of our technology outsourcing to various countries that may be a friend today but a foe tomorrow, and perhaps vice versa. As a case in point, consider the recent activity in Vietnam, which in a few decades has gone from a war zone to a major commercial center.

Security and Operations

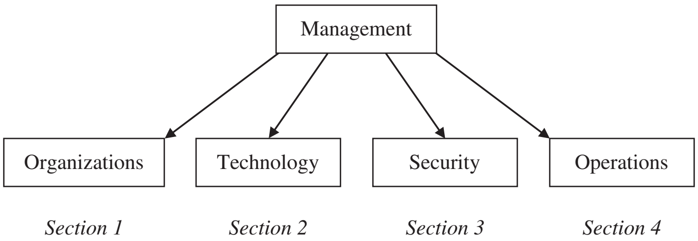
In addition to protecting people and facilities, managers have the responsibility to protect the confidentiality, integrity, and availability (known as CIA) of information resources and the infrastructure that enables these attributes. There are safeguards for computer systems, networks, mobile devices, databases, and the like. However, managers need to assess the company infrastructure and the threat risks to the infrastructure. They must determine the vulnerabilities of their infrastructure to threats and determine potential exposure and probable loss in the event of an attack or disaster.

Managers need to make plans for implementing security measures and formulate contingencies in case of a security breach. They must oversee the implementations of security measures and personnel training programs and evaluate the implementations in an iterative cycle to ensure continuous vigilance and improvements. They must do all of these things in the midst of planning projects according to budgets and making their scheduled deadlines. The broad categories of tasks that managers must perform show just how much a manager's responsibilities have expanded beyond the traditional management of employee performance and asset utilization. Organizations have flattened since the 1980s, which means that managers must do more with less—and there seems to be no end in sight for this expectation.

Running daily security operations includes monitoring for and defending against security attacks. Intrusion detection systems are available to indicate attempts at finding vulnerabilities and attempts to exploit them. There are procedures that managers follow to determine how security incidents may have occurred after the fact. Managers determine corrective actions that may need to be taken, as well as how to preserve evidence. Managers are also interested in techniques and technologies that can be used to predict attacks and disasters in an effort to avoid them.

Textbook Organization

To help answer questions that many, if not most, managers have about how to stay viable in this dynamic technological world, we have developed a textbook to arm managers with answers to the most critical questions and to provide them with references to more in-depth study in areas where they may need to specialize. As such, our textbook is organized as seen in the following diagram, covering organizations and the rules of law and policies, an introduction to technologies for managers, an introduction with emphasis on security and security initiatives, and finally, a view of security operations and strategic aspects of security that may lay on the horizon:



- ✓ *Section 1* introduces the legal, organizational, and informational structure of companies. This beginning frames the managerial context and discusses common constraints that confront managers in conducting their business securely.
- ✓ *Section 2* provides an orientation of technologies to a management audience. It provides a high-level summary of technical details that underlies security threats and security measures that concern managers.
- ✓ *Section 3* covers, at the conceptual level, computer, network, and information security to protect their confidentiality, integrity, and availability.
- ✓ *Section 4* explores how to monitor information and systems, handle security incidents, and manage security behaviors. This section also posits what lies on the security horizon.

Textbook Content

The field of information security is heavily published, and most of the publications are divided along either technical or administrative lines. Technical publications include resources to target security of information systems (IS) such as computers and networks aimed at implementations and implementers. Administrative publications cover policies, security models, standards, and operations aimed at regulators, auditors, and government agencies. We believe that a comprehensive information security resource for managers should introduce a broad range of topics that are not targeted at a particular security certification or a given government agency. Our position is that once managers in commercial enterprises understand security in general, they can then dive into the security domain knowledge for their industry or agency.

Given these assumptions, we introduce managers to technologies including operating systems, applications, databases, and networks, while digging into the means used to secure these systems. We introduce trends that include advances in mobile technologies, along with more traditional fixed-site systems. In addition to these technical aspects of security, we provide coverage of regulations and applicable security and employment law, but not at a level where the *forest is lost among the trees*.

In this textbook, we include coverage of these important concepts, but at a level that is appropriate for managers who oversee technology implementations and people who work with technology. We also cover security behavior in organizations because the research literature on security continues to point to the human element (sometimes called the *weakest link*) as one of the most important aspects of information security, and yet this continues to be treated sparsely in terms of what to do about this problem, especially as it relates to what is known as the *knowing–doing gap*—that is, knowing better, but not doing better. With our textbook, we present a practical and yet comprehensive publication for knowledge-work managers that includes all of these aspects.

Knowledge Scaffolding

A typical textbook is usually organized topically. Topical organization is useful for rote memorization of a topic or for referencing information later. Our approach is different. Pedagogically, we designed this textbook for academic programs in such areas as management information systems, information systems management, and information science, but it should also be applicable to management and security readership more generally and should be appealing to all those who are concerned about organizational information security. It is not written in the style of a reference manual or a guide to a particular security certification.

To that end, we utilize an incremental development method called *knowledge scaffolding*—a proven educational psychology technique for learning subject matter thoroughly. Knowledge scaffolding means that certain materials are presented in iterative chunks. A chunk is presented with other chunks to flesh out an idea, and then the ideas are presented again in different contexts (and in different chapters) to develop a deeper and broader understanding of the topic in relation to the other topics for a holistic understanding, as well as to reinforce learning through an elaborative rehearsal process.

We chose this approach because there are plenty of reference materials generally available for readers and students who are studying information security, including those that are freely available on the Internet, and those resources are certainly valuable and needed during referential lookups or general knowledge acquisition. Our goal with this textbook is to help readers learn about managing information security from the ground up and to reinforce the learning as they read on. This textbook is also organized to first concentrate on general management issues and then gradually evolve into more technical content. This should assist readers with properly framing the technical information into a managerial perspective.

Learning Approach and Objectives

We adopt a Gestalt approach to the presentation of information in our textbook. The essence of this approach is to create greater insight and understanding through the presentation of "new relationships" that emerge from situating familiar information in different contexts. This is an especially effective technique for those who bring world experience to a learning activity and then are given a variety of frames in which to view the information and their experiences differently.

Who Will Benefit from This Textbook?	**What They Will Learn:**
✓ Students of Security and Management ✓ Managers and Project Leads ✓ Systems and Software Developers ✓ Product and Technical Directors ✓ Information Architects ✓ Business Analysts ✓ Human Resource Policy and Standards Coordinators ✓ Strategic Planners ✓ Systems and Solutions Designers ✓ Technical Consultants ✓ Information and Security Officers	❑ How to use security principles in designs to improve the security of systems. ❑ How to effectively manage security behaviors. ❑ How to improve decision making and problem solving about security issues. ❑ How to evaluate and justify security technology selections and designs. ❑ How to improve returns on security technology investments. ❑ How to establish organization-wide security of information systems that align technical with business needs and goals. ❑ How to apply the appropriate security tools effectively. ❑ How to plan for existing and future needs and emerging security issues.

Looking Forward

In this textbook, we want to construct a bird's-eye view of the state of the art in security management and provide a glimpse of what may lay ahead in the evolution of—or maybe even revolution in—information security. This is important because we are on the verge of a paradigm shift (to borrow Thomas Kuhn's salient term from his seminal book, *The Structure of Scientific Revolutions*). The shift is occurring on at least three levels: (1) there is an increased emphasis on understanding and managing human security behaviors, (2) there is a need to incorporate social media and new communications technology in the security rubric, and (3) there is an evolution of semantic integration and fusion systems used in security infrastructure, modeling, and prediction.

In our endeavor to provide a bird's-eye view of the state of the art, we will (1) elucidate new approaches to solving real-world information security problems, such as how to address organizational security behaviors, (2) contrast competing paradigms and approaches to security problem solving and decision making, using technology as a tool and a technique, (3) highlight promising directions, and (4) prompt constructive thought around contemporary business and technological security themes.

Additional Information About This Textbook

This textbook focuses special attention on managing information, systems, and people securely. Each chapter develops key concepts and presents issues that managers should know in order to effectively oversee their departments. Because the emphasis is on management of information resources, it provides mainly the "what" aspects of information systems and technologies, and suggests more in-depth coverage of "why" certain practices or procedures are used. It will provide some insight into features and functions of security technologies and techniques and will develop some bridge knowledge into security threats and the countermeasures that managers and security professionals use to help prevent or neutralize them. We begin our textbook with organizational considerations and then move into more technical topics. The more technical aspects of security provide a high-level view of the procedural and technological features of operations and management in an information security context. We hope you find this book a useful resource for learning, as well as a reference throughout your management and information security career.

In the chapters that follow, you will see "**In Focus**" points. These are important topics that should spark you to do some reflective thinking and suggest further research on a particularly important topic. At the end of each chapter, you will also find questions and exercises to do in a section titled "**Think About It**." The exercises will test your knowledge from your readings. There are also some extended study questions to ponder in a broader context that will require that you do some critical thinking about the materials you have read. You may need to investigate those key points using other readily available resources.

Additional Resources for Instructors

Answers to end of chapter questions and a PowerPoint Image Bank that contains key images from the text are available for instructor download at go.jblearning.com/Workman.

Acknowledgments

The authors would like to thank the following colleagues for their valuable feedback on our textbook:

Hamid R. Arabnia, PhD, University of Georgia

William H. Bommer, PhD, California State University at Fresno

Darrell E. Burke, PhD, University of Alabama at Birmingham

Kathy Chudoba, PhD, Utah State University

Richard Ford, PhD, Florida Institute of Technology

Mike Gancarz, Vice President, Bank of America

Misook Heo, PhD, Duquesne University

Guido Hertel, PhD, University of Muenster, Germany

Peter Horn, PhD, International School of Management, France

Larry Hyde, CISSP, The Hyde Group

Ryan Long, JD, U.S. Department of Defense

E. Eugene Schultz, PhD, Late of University of California at Berkeley

Eugene H. Spafford, PhD, Purdue University

Detmar W. Straub, PhD, Georgia State University

Nikos Tsianos, PhD, University of Athens, Greece

A special thanks to E. Eugene (Gene) Schultz, who tragically passed away in October 2011.

Thank you also to the Editorial and Production teams at Jones & Bartlett Learning: Tim Anderson, Senior Acquisitions Editor; Amy Bloom, Managing Editor; Chris Will, Vice President, Professional Sales and Business Development; Alyssa Lawrence, Production Assistant; and all the Jones & Bartlett Learning staff who diligently worked with us behind the scenes.