

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

Preface xv

SECTION ONE What Should Managers Know About Security Policies and Procedures? 1

CHAPTER 1 Introduction to Information Security 3

Technological and Behavioral Security Issues	4
Organizational Governance	4
Security, Cyber Crime, and Costs	5
Management Duties, Responsibilities, and Threats	7
Assessing and Planning	7
Financial Evaluations	8
Attacks, Monitoring, and Recovery	9
Reasons Why “They” Attack “Us”	10

CHAPTER 2 Corporations and the Rule of Law 15

Legal Organizational Structure	16
Accountability, Responsibility, and Law	16
Roles of Corporate Trust and Regulation	18
Formal Project Undertakings	19
Power and Organizational Structure	21
Fiduciary Responsibilities	24
Fiduciary Duties and Legal Ethics	24
Law and Ethics Intersection	25
Legal and Ethical Consciousness	26
Law and Enforceable Security Policies	28
Enforceable Security Policies	29
People and Policies—The Weakest Link	29
CHAPTER SUMMARY	30
THINK ABOUT IT	31
KEY CONCEPTS AND TERMS	32

CHAPTER 3 Management, Security Law, and Policies 35

The Management Discipline	36
Management Initiatives and Security	37

Information Security Management	37
Information Security Management Life Cycle	39
Security Law and Cyber Knowledge Work	40
Security, Employment Law, and Policies	40
Virtual Work, Security, and Privacy	43
Intellectual Property Law	45
Trade Secrets	45
Patents	46
Copyrights	46
Employee Surveillance and Privacy	47
Video Surveillance	47
Privacy and Policy	48
Surveillance and Organizational Justice	49
Cyber Law and Cyber Crime	49
International, Federal, and State Cyber Law	49
Employee Behavior and Cyber Law	50
Corporate Espionage	51
Forensics	52
What Constitutes Evidence?	52
Cyber Crime Evidence	53
Cyber Law and Cyber Crime Issues	53
CHAPTER SUMMARY	54
THINK ABOUT IT	54
KEY CONCEPTS AND TERMS	55

CHAPTER 4 Security Regulations and Governance 59

Governance and U.S. Regulations	60
Gramm-Bliley-Leach Act (GBLA)	61
U.S. Fair and Accurate Credit Transactions Act (FACTA)	64
U.S. Sarbanes–Oxley Act (SOX)	64
OMB Circular A-123 (Revised)	65
Government Information Security Reform Act of 2000	65
HIPAA and Health Insurance Reform	66
Non-U.S. and International Governance	67
U.K. Combined Code on Corporate Governance	67
CCCG and Turnbull Guidance	68
Basel II	69
U.K. Data Protection Act	69
European Union and Other Privacy Protections	70
Canadian PIPEDA	71
Asian APEC Data Privacy Subgroup	72
Management and Governance	72
Governance and Security Programs	73

Enactment of Security Programs	74
Analyzing the Problem and Managing IT	75
CHAPTER SUMMARY	76
THINK ABOUT IT	76
KEY CONCEPTS AND TERMS	77

CHAPTER 5 Security Programs: Risk Assessment and Management 79

Risk Assessment and Management Overview	80
Security Program Overview	81
Risk Assessment Overview	81
Risk Mitigation Overview	82
Risk Determination and Control Frameworks	83
ITIL / ITSM	84
COBIT	85
ISO 27K IT Security Control Selection	86
NIST 800-53	87
Risk Management Frameworks	89
OCTAVE	90
NIST 800-30	91
Using Frameworks for Implementing Plans	94
CHAPTER SUMMARY	95
THINK ABOUT IT	95
KEY CONCEPTS AND TERMS	96

CHAPTER 6 Managing Organizations Securely 99

Security Management Overview	100
Information and Systems Security Infrastructure	101
Information Assets: Classification and Architecture	102
Security Policies and Models	102
Stances and Countermeasures	104
Risk Assessment and Management	105
Risks and Countermeasures	105
Hoping for the Best, Planning for the Worst	108
Trusted Computing Base Versus Common Criteria	109
Evaluation and Certification	110
Monitoring and Security Policies	111
Monitoring as a Policy	112
Information Collection and Storage	113
Monitoring and Organizational Justice	114
Surveillance and Trust	115
CHAPTER SUMMARY	116
THINK ABOUT IT	117
KEY CONCEPTS AND TERMS	118

SECTION TWO Technology Orientation for Managers 121

CHAPTER 7 Data, Information, and Systems 123

Information Systems	124
The Nature of Data and Information	125
IS Operations, Tactics, and Strategies	125
Information Integration and Exchange	128
Databases	129
Relational Databases	130
Relational Databases and Maintaining Data Integrity	132
Data Warehouses	134
Extract-Transform-Load (ETL)	135
Distributed Systems and Information	136
Globalization and Information Exchange	136
Distributed Systems Architecture	138
Markup: HTML and XML	140
Parsing Markup	142
RDF and Ontology Markup	143
Active Semantic Systems	144
Agent Frameworks and Semantic Fusion	145

CHAPTER SUMMARY 147

THINK ABOUT IT 148

KEY CONCEPTS AND TERMS 149

CHAPTER 8 Programming Concepts 151

Program Creation	152
Programming Logic and Syntax	152
Operations, Expressions, and Tasks	155
Software Construction	157
Code-Level Design: Coupling	158
Code-Level Design: Cohesion	160
Rapid Application Development Tools	165
IDE, Wizards, and Toolkits	167
Native Programming Environments	167

CHAPTER SUMMARY 168

THINK ABOUT IT 168

KEY CONCEPTS AND TERMS 169

CHAPTER 9 Applications Programming 171

Object-Oriented Software	172
Objects and Object Features	173
The Nature of Software Objects	174

Abstractions and Complex Data Types	176
Object Composition	177
OOP and Applications	178
Database Interaction	180
SQL Overview	181
Software and RDBMS Concurrency	183
Distributed Systems	185
Web Applications	186
Web Application Processing	187
JAVA Servlets	189
Distributed Web-Based Systems	190
CHAPTER SUMMARY	192
THINK ABOUT IT	192
KEY CONCEPTS AND TERMS	193

CHAPTER 10 Computer Operating Systems 195

Operating Systems: An Introduction	196
Systems and Software	196
What Do OS Do?	198
Windows and UNIX (Linux)	199
Digital Architecture	201
Hardware Components	201
Binary Logic and Computer Hardware	202
Hardware Logic and Software Instructions	204
UNIX-Based Operating System Functions	205
OS Features	205
UNIX-Based (Including Linux and MAC/OS) Processes	206
The UNIX-Based File System	212
Disk Memory Management	216
UNIX System Input–Output (I/O) and Device Drivers	218
Microsoft Windows Operating System	220
Windows as a Reference Example	221
Windows Microkernel, Memory, and I/O Management	223
Windows Processes and Security Management	224
Microsoft Registry	225
CHAPTER SUMMARY	226
THINK ABOUT IT	227
KEY CONCEPTS AND TERMS	228

CHAPTER 11 Networks and Addressing 229

The ISO/OSI and TCP/IP	230
Layered Architecture	231
Inter-Networking	232

Packet and Circuit Switching	233
Network Topologies	234
Devices and Addressing	236
IP Addressing	237
Subnetworks	238
IPv4 Versus IPv6	240
IPv6 Address Groupings and Uses	241
IPv6 Address Configuration	242
Network Connections Summarized	243
Data Link Layer Connectivity	244
Communications Facilities	245
CHAPTER SUMMARY	247
THINK ABOUT IT	247
KEY CONCEPTS AND TERMS	248

CHAPTER 12 **Protocols and Routing** **249**

Link-Point Networking	250
Physical Connections	250
Carrier Sense Multiple Access with Collision Detection (CSMA/CD)	251
Transiting Data: Egress and Ingress	252
Internet Control Message Protocol (ICMP)	253
Encapsulation and the TCP/IP Protocol Stack	254
Headers and Name Resolution	255
Address Resolution Protocol (ARP)	257
End-Point Networking	258
Services and Sockets	258
Transport and Sessions	261
Applications Layer Protocols	263
Routing Data	266
Routes and Route Tables	266
Routing Protocols	269
CHAPTER SUMMARY	270
THINK ABOUT IT	271
KEY CONCEPTS AND TERMS	272

SECTION THREE **Computer and Network Security** **273**

CHAPTER 13 **Information Systems Security** **275**

Social Interactions and Security Implications	276
Mobility and Threats	276
Distributed Work and Threats	277
Interconnectivity and Threats	278
Security Countermeasures and Complications	279

Broad Attack Classifications and Examples	280
Information System Attack Examples	280
Social Engineering Attack Examples	282
Mobile Device Attack Examples	283
Infosec	284
Threat Awareness and Risk Management	285
Administrative, Technical, and Physical Controls	286
Managing Organization Members Securely	287
Perceptions of Control and Security	287
Sins of Omission	288
Sins of Commission	289
Social Influences and Legalistic Perceptions	290
CHAPTER SUMMARY	291
THINK ABOUT IT	292
KEY CONCEPTS AND TERMS	293

CHAPTER 14 **Computer Security** **295**

Hosts and Security—A Windows Example	296
Microsoft Active Directory	296
Windows Security Access Controls	297
Windows Service and Process Security	300
Access Management Framework in Windows	301
Windows Version Security Differences	303
Getting Past OS Security Features	305
Circumventing Security (in Windows and Other OS)	306
Host Attack Classifications and Examples	309
Monitoring Attacks—Tools of the Trade	311
Monitoring Host Attacks	311
Intrusion Detection Systems	312
Assessing Systems Security	314
Assessing the Information and System	314
Vulnerability Testing	315
Test Reports and Recommendations	316
Hardening Systems	317
Ensuring a Trusted Configuration	318
Password Protections	319
User Authentication	320
Biometrics	321
Biometrics Acceptance	321
Biometric Security Process and Information Protection	322
Biometrics and Errors	323
Biometric Errors and Technology	323
Biometric Frontiers in Computer Security	325

Secure Software and Systems SDLC	326
Secure Systems Development	326
Configuration Management	328
CHAPTER SUMMARY	329
THINK ABOUT IT	330
KEY CONCEPTS AND TERMS	331
CHAPTER 15 Network Security	333
Protecting Networks from Being Undermined	334
Threats and Network Security	334
Attacks and Tools	336
Some Attack Classifications and Examples	338
Know Thy Enemy's <i>Modus Operandi</i>	339
Reconnaissance and Attack Preparations	339
Enumeration	340
Sorting Out the Targets and Gaining a Foothold	341
Target Exploitation	342
Network Security Issues—Link to Link	342
Connection Layer Security Issues	342
Link Layer Security Issues	343
ARP, Neighbor Discovery, and Poisoning	344
Internet Layer Security Issues	345
Network Security Issues—End to End	346
ICMP Security Issues	346
Layer 4 (TCP/UDP) Security Issues	347
Port Attacks and SYN Floods	348
Network Countermeasures	350
Limiting and Controlling Information Releases	351
Protecting Zone Transfers and Thwarting DNS Spoofing	352
Using Proxies and VPNs	353
CHAPTER SUMMARY	354
THINK ABOUT IT	354
KEY CONCEPTS AND TERMS	355
CHAPTER 16 Cryptography Uses and Firewalls	357
Cryptography in Use	358
Who Knows Whom: X.509 Certificates	358
IPSec Implementation	359
IPSec Example	360
SSL/TLS	361
Virtual Private Networks (VPNs)	362
Firewall Systems	366
Stateless Screening Filters	366
Stateful Packet Inspection	367

Circuit Gateway Firewalls	369
Application-Layer Firewall	369
Bastion Hosts	370
Firewall Architecture	372
"Belt and Braces" Architecture	372
Screened Subnet Architecture	374
Ontology-Based Architecture	375
CHAPTER SUMMARY	377
THINK ABOUT IT	377
KEY CONCEPTS AND TERMS	378

CHAPTER 17 **Cryptography—And How IT Works** **381**

Cryptography Overview	382
Cryptographic Concepts	382
Generating a Simple Cipher Code	384
Breaking a Simple Cipher Code	386
Ciphertext Dissection and "S" Boxes	387
Cryptography and Security Goals	387
Symmetric Cryptography	391
Symmetric Ciphers and Keys	391
Substitution, Transposition, and Permutation	392
Modern Symmetric Ciphers	396
Key Issues with Symmetric Cryptography	398
Asymmetric Cryptography	399
Public Keys and Asymmetric Cryptography	400
Beyond Encrypting Messages	401
Key Distribution and PKI	402
Public Key Algorithms: RSA as an Example	403
CHAPTER SUMMARY	406
THINK ABOUT IT	406
KEY CONCEPTS AND TERMS	407

CHAPTER 18 **Web Applications Security** **409**

Web-Based Versus Web-Enabled Applications	410
A Definition of Web Applications	410
Client-Server Web Applications and Security	411
Web Services and Cloud Computing	412
Securing Web Servers	413
Web Application Threats	414
Protections for Web Servers	416
Authentication	416
Password Protections	417
Authorization	418
Input Validation	418

Session Management	419
Web Services and Security	421
Protecting Web Content	422
CHAPTER SUMMARY	422
THINK ABOUT IT	423
KEY CONCEPTS AND TERMS	424

SECTION FOUR Managing Organizations Securely 425

CHAPTER 19	Configuration Management	427
	CM and Computer Security Procedures	428
	CM and Management Frameworks	428
	Managing Configurations	430
	Security Configuration Management	431
	Security Management	432
	Security Management Planning—System Level	433
	Configuring to a Secure State	435
	Managed Enterprises	437
	Checklist Groups	438
	Extended Guidelines	439
	DISA STIGs	439
	Private Industry Baseline Security	440
	Center for Internet Security Benchmarks	440
	Maintaining the Secure State	441
	Controlling Changes	441
	Conducting a Security Impact Analysis	443
	Certification and Accreditation	443
	CHAPTER SUMMARY	444
	THINK ABOUT IT	445
	KEY CONCEPTS AND TERMS	445

CHAPTER 20	Operations	447
	Maintaining Operations	448
	The SDLC and Security	448
	Planning: Failures Are a Rule, Not an Exception	450
	Maintaining Operational Capabilities	451
	Operational Continuity	452
	Monitoring Systems and Networks	452
	Auditing Systems and Networks	454
	Operations Centers and Contingencies	455
	Cloud Computing	456
	Security Incidents	457
	Handling Inevitable Incidents	458
	Reporting Security Incidents	459

Collecting and Preserving Evidence	460
Computer Forensics and the Law	462
Cyber Stalking and Harassment Incidents	463

CHAPTER SUMMARY 465**THINK ABOUT IT 465****KEY CONCEPTS AND TERMS 466****CHAPTER 21 Managing Security Behavior 469**

Organizational Behavior	470
Behavior and Control	470
Behavior Modification	471
Organizational Security Behaviors	472
Malicious Outsiders	472
Malicious Insiders	473
Non-malicious Unintentional Insider Omission	474
Non-malicious Intentional Insider Omission	474
Management of Omission Behaviors	477
Responding to the Unintentional Omission	477
Responding to the Intentional Omission	478
Leading by Example	479
Contravention Behaviors, Theory, and Research	479
Attacker Motivation, Personality, and Behavior Theory	480
Entertainment and Status	480
Ideology and Social Acceptance	481
Neuroticism, Impulse, and Exploitation	481
Management of Contravention Behaviors	482
Responding to the Outside Attacker	482
Responding to the Inside Attacker	484
Ethics and Employee Attitudes Toward the Law	484

CHAPTER SUMMARY 486**THINK ABOUT IT 486****KEY CONCEPTS AND TERMS 487****CHAPTER 22 Modeling and Predicting Attacks 493**

Game Theory and Predictive Models	494
Inductive Predictions	494
Deductive Predictions	496
Game Theory and Attack Modeling	497
Reasoning and Inference	499
Reasoning Systems	499
Ontology and Epistemology	500
Inference and the Ontological to Epistemic Transformation	502
Heuristics and Decision Systems	505
Reasoning: Discrete Versus Equivocal Problems	505
Synthetic Heuristics	506

Issues with Synthetic Heuristic Systems	508
Combining Techniques	509
Heuristic Biases and Security Planning	511
Decisions, Naïve Theories, and Biases	511
Interactions of Biases and Framing Effects	514
Biases, Framing Effects, and Security Decisions	515
CHAPTER SUMMARY	516
THINK ABOUT IT	516
KEY CONCEPTS AND TERMS	517

CHAPTER 23 Adaptive Systems Security 521

Biologically Inspired Security	522
Self-Healing Systems	522
Damage and Danger	523
Trusted Security Kernels	524
Social Systems	526
Socially Inspired Security	526
Social Systems and Security Adaptation	528
Collective Agency, Availability, and Integrity	530
Socio-Biologically Inspired Security Systems	530
Novelty as Potential Danger	531
Socio-Biological Behavior as Goal-Directed Behavior	533
Adaptive Synthetic Systems	534
Challenges for Mobile Networks and Adaptive Systems	535
CHAPTER SUMMARY	537
THINK ABOUT IT	537
KEY CONCEPTS AND TERMS	538

CHAPTER 24 Security Horizons: Issues for Managers 541

Localized Security Issues	542
The Changing Technology, Security, and Attack Landscape	542
Advanced Technologies, Threats, and Attacks	543
Security, Processes, and Priorities	544
Security, Situations, and Behavior	545
Biometric Trends	547
Political and Behavioral Issues in Security	547
Legislation and Global Security	548
Globalization and Information Exposure	549
Security and Ethical Governing	551
CHAPTER SUMMARY	552
THINK ABOUT IT	552
KEY CONCEPTS AND TERMS	553

Index	555
--------------	------------

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.

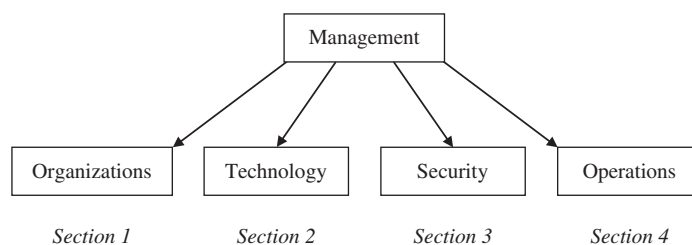
Managers need to make plans for implementing security measures and formulate contingencies in case of a security breach. They must oversee the implementations of security measures and personnel training programs and evaluate the implementations in an iterative cycle to ensure continuous vigilance and 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	❑ How to use security principles in designs to improve the security of systems.
✓ Managers and Project Leads	❑ How to effectively manage security behaviors.
✓ Systems and Software Developers	❑ How to improve decision making and problem solving about security issues.
✓ Product and Technical Directors	❑ How to evaluate and justify security technology selections and designs.
✓ Information Architects	❑ How to improve returns on security technology investments.
✓ Business Analysts	❑ How to establish organization-wide security of information systems that align technical with business needs and goals.
✓ Human Resource Policy and Standards Coordinators	❑ How to apply the appropriate security tools effectively.
✓ Strategic Planners	❑ How to plan for existing and future needs and emerging security issues.
✓ Systems and Solutions Designers	
✓ Technical Consultants	
✓ Information and Security Officers	

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.

