
Team LiB

Current Security Management & Ethical Issues of Information Technology

Rasool Azari

IRM Press

Current Security Management & Ethical Issues of Information Technology

edited by

Rasool Azari
University of Redlands, USA

IRM Press
Publisher of innovative scholarly and professional information technology titles in the cyberage
Hershey • London • Melbourne • Singapore • Beijing

Acquisitions Editor: Mehdi Khosrow-Pour
Senior Managing Editor: Jan Travers
Managing Editor: Amanda Appicello
Copy Editor: Alana Bubnis
Typesetter: Jennifer Wetzel
Cover Design: Michelle Waters
Printed at: Integrated Book Technology

Published in the United States of America by
IRM Press (an imprint of Idea Group Inc)
701 E. Chocolate Avenue, Suite 200
Hershey PA 17033-1240
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@idea-group.com
Web site: http://www.irm-press.com

and in the United Kingdom by
IRM Press (an imprint of Idea Group Inc)
3 Henrietta Street
Covent Garden
London WC2E 8LU
Tel: 44 20 7240 0856
Fax: 44 20 7379 3313
Web site: http://www.eurospan.co.uk

Library of Congress Cataloging-in-Publication Data

Azari, Rasool.
Current security management & ethical issues of information technology / Rasool Azari.
p. cm.
ISBN 1-931777-43-8 (soft cover) -- ISBN 1-931777-59-4 (ebook)
1. Computer security. 2. Computer networks--Security measures. I. Title.
QA76.9.A25A93 2003
005.8--dc21

2002156229

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

New Releases from IRM Press

- **Multimedia and Interactive Digital TV: Managing the Opportunities Created by Digital Convergence**/Margherita Pagani
  ISBN: 1-931777-38-1; eISBN: 1-931777-54-3 / US$59.95 / © 2003
- **Virtual Education: Cases in Learning & Teaching Technologies**/ Fawzi Albalooshi (Ed.), ISBN: 1-931777-39-X; eISBN: 1-931777-55-1 / US$59.95 / © 2003
- **Managing IT in Government, Business & Communities**/Gerry Gingrich (Ed.)
  ISBN: 1-931777-40-3; eISBN: 1-931777-56-X / US$59.95 / © 2003
- **Information Management: Support Systems & Multimedia Technology**/ George Ditsa (Ed.), ISBN: 1-931777-41-1; eISBN: 1-931777-57-8 / US$59.95 / © 2003
- **Managing Globally with Information Technology**/Sherif Kamel (Ed.)
  ISBN: 42-X; eISBN: 1-931777-58-6 / US$59.95 / © 2003
- **Current Security Management & Ethical Issues of Information Technology**/Rasool Azari (Ed.), ISBN: 1-931777-43-8; eISBN: 1-931777-59-4 / US$59.95 / © 2003
- **UML and the Unified Process**/Liliana Favre (Ed.)
  ISBN: 1-931777-44-6; eISBN: 1-931777-60-8 / US$59.95 / © 2003
- **Business Strategies for Information Technology Management**/Kalle Kangas (Ed.)
  ISBN: 1-931777-45-4; eISBN: 1-931777-61-6 / US$59.95 / © 2003
- **Managing E-Commerce and Mobile Computing Technologies**/Julie Mariga (Ed.)
  ISBN: 1-931777-46-2; eISBN: 1-931777-62-4 / US$59.95 / © 2003
- **Effective Databases for Text & Document Management**/Shirley A. Becker (Ed.)
  ISBN: 1-931777-47-0; eISBN: 1-931777-63-2 / US$59.95 / © 2003
- **Technologies & Methodologies for Evaluating Information Technology in Business**/Charles K. Davis (Ed.), ISBN: 1-931777-48-9; eISBN: 1-931777-64-0 / US$59.95 / © 2003
- **ERP & Data Warehousing in Organizations: Issues and Challenges**/Gerald Grant (Ed.), ISBN: 1-931777-49-7; eISBN: 1-931777-65-9 / US$59.95 / © 2003
- **Practicing Software Engineering in the 21st Century**/Joan Peckham (Ed.)
  ISBN: 1-931777-50-0; eISBN: 1-931777-66-7 / US$59.95 / © 2003
- **Knowledge Management: Current Issues and Challenges**/Elayne Coakes (Ed.)
  ISBN: 1-931777-51-9; eISBN: 1-931777-67-5 / US$59.95 / © 2003
- **Computing Information Technology: The Human Side**/Steven Gordon (Ed.)
  ISBN: 1-931777-52-7; eISBN: 1-931777-68-3 / US$59.95 / © 2003
- **Current Issues in IT Education**/Tanya McGill (Ed.)
  ISBN: 1-931777-53-5; eISBN: 1-931777-69-1 / US$59.95 / © 2003

Excellent additions to your institution's library!
Recommend these titles to your Librarian!

To receive a copy of the IRM Press catalog, please contact (toll free) 1/800-345-4332, fax 1/717-533-8661, or visit the IRM Press Online Bookstore at: [http://www.irm-press.com]!

Note: All IRM Press books are also available as ebooks on netlibrary.com as well as other ebook sources. Contact Ms. Carrie Skovrinskie at [cskovrinskie@idea-group.com] to receive a complete list of sources where you can obtain ebook information or IRM Press titles.

Current Security Management & Ethical Issues of Information Technology

Table of Contents

Preface

As *Time* magazine proclaimed 20 years ago, "The 'information revolution' that futurists have long predicted has arrived…America will never be the same. In a larger perspective, the entire world will never be the same" (January 3, 1983, p. 14). Since the dawn of civilization our lives have been improved and sometimes also uprooted by evolving technologies, but there is no precedent to the explosive pace of innovations experienced in this time and age, and we are told by experts that this is just the beginning.

The information technology is a major force of this ongoing revolution. What started with the cumbersome, oversized dinosaurs of the first generation computers has mushroomed into the age of mobile computing, the Internet, and the open access worldwide networks. Information technology has increased productivity, shortened the product life cycle, diminished the importance of distance, and globalized markets and economies. New communication technologies centered around information technologies are linking markets, institutions, and populations all over the globe and are radically altering our lives and work. Increased use of technology and the development of e-business are transforming established organizational patterns and are profoundly changing current business structures. Products and services are becoming more and more knowledge and information dependent. The labor force composition has reversed from being seventy percent blue-collar and farm workers into seventy percent white-collar and service providers within the last century. Nearly sixty percent of the American gross national product comes from information and knowledge sectors; some experts even argue that these knowledge assets are at least as important as physical and financial assets in ensuring the survival of organizations (Laudon, 2002).

Because of the need for new and different organizational infrastructures, management is pressured to reconsider its purpose and its methods of operation. Information technology not only challenges and alters the way we produce new goods and services, but it also triggers far-reaching change in institutional arrangements,

social norms, and cultural values. It is playing a crucial role in economic well being and introducing a form of relationship among societies and nations never experienced before**.** Even educational institutions are being revolutionized through distance learning by the new computer-mediated communication technology and Internet-based support.

In addition to adjusting to these changes, societies will also have to come to terms with the unprecedented speed with which change occurs. And this pace is accelerating because the increasingly powerful technologies facilitate the exponentially multiplying pool of knowledge and vice versa. 'Faster, cheaper, smaller' are more than slogans for the information technology. The speed and reach of electronic transmission and distribution and the increasing computing power of microprocessors allow new technologies to reach a quarter of all households in less than a decade, compared to the span of two generations half a century ago. As Alfred Chandler, a Harvard Business historian argues, the driving force in the market is now the economics of speed, not the economies of scale (Grupp, 2001). Speed has become a source of competitive advantage.

These dizzying developments bring an array of unknowns. In uncharted territories, people are faced with questions of law, ethics, and security, brought on by the unfamiliar circumstances created by the new technologies. The astonishing possibilities promised tend to obscure the sobering fact that technology is, and always has been, like a two-sided sword — it may cut both ways. Its destructive potential can outdo its beneficial powers, because it is exactly those marvelous benefits which make possible the potential risks. On the one hand, people are getting closer to each other but on the other hand they are becoming more virtual, anonymous, and impersonal. While extensive use of networks and the Internet, easy access to technology, and advances of wireless telecommunication all raise the likelihood of progress and growth and can benefit both organizations and individuals, they simultaneously raise risks of computer hacking and criminality. The concurrent growth in interdependence, anonymity, and location independence all add to this vulnerability.

As populations become more and more comfortable with the extensive use of networks and the Internet, as our reliance on the knowledge-intensive technology grows, and as progress in the computer software and wireless telecommunication increases accessibility, "there will be a higher risk of unmanageable failure in either physical or social systems that underpin survival…the spread of information technology makes it easier to violate basic privacy or civil rights and to engage in criminal practices ranging from fraud and theft to illegal collusion" (OECD, 2001, p.15). The increasing importance of information technology for production, storage, and distribution of our scarce resources demands that we ensure the reliability, accuracy, and security of our systems and pay special attention to the ethical issues involved.

The ethical issues raised by information technology relate, among others, to privacy, the ownership of information, and intellectual property rights. What is meant by property rights? How can we protect privacy? What are common security weak-

nesses? How is network security defined? What is the social contract? What is responsibility? What does corporate and social responsibility mean? How does information technology create ethical problems? How does information technology cause change in society and vice versa? Can we reduce the digital divide? There are no easy answers to these or other related questions. The chapters in this book try to address some of the challenges. Most of these topics relate directly or indirectly to questions of risk. To decrease the systems' vulnerability and to minimize risks of breaches of security and computer crimes, we need to develop policies and procedures and design control structures that incorporate the vigilance necessary to stay abreast of the changing technology and its demands for security. Embracing security management programs and including them in the decision making process of policy makers helps to detect and surmount the risks with the use of new and evolving technologies. Raising awareness about the technical problems and educating and guiding policy makers, educators, managers, and strategists is the responsibility of computer professionals and professional organizations.

However, no matter how secure systems may be, insecurities will remain. People are constantly concerned with the search for more security in their lives, homes, jobs, and relationships. How secure is secure? Technology alone is not the solution. As Schneier (2000) put it: "If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology." Security is not only about software packages, good encryption, and symptomatic remedies.

In an increasingly interdependent world in which our decisions have greater significance to others, moral standards must be critically re-examined. It is more essential to include everyone affected in the decision making process. It is important to move away from compartmentalized thinking that fails to recognize all perspectives involved and thereby does not consider the consequences of our actions. Adhering to a holistic approach not only fosters an agile and alert mind necessary to constructively deal with the many upheavals, disruptions, and changes stemming from the new technologies, it also facilitates the responsible thinking needed in a globalized world. If ethical consideration and social responsibility do not drive technological advance, human misery may be increased. Since technology is used in all of our institutions, "in a social context rich with moral, cultural, and political ideas," (Johnson, 2001) and thus directly and substantially affects all of our lives, it is the responsibility of all businesses, governments, educational institutions, and citizens to exert our social responsibility in steering its moral course.

Securing and harnessing the powers of present and especially future technologies is and will stay a formidable task that requires concerted efforts. Information and education will be a major asset to the achievement of this goal.

This book contributes by encouraging and furthering the dialogue. It brings together ideas and expertise from different fields. It is a response to the many questions raised by the rapid development of information technology that concern security management and ethical issues. It seeks to shed some light on the prob-

lems society is facing because of these technological changes and it suggests some solutions.

STRUCTURE OF THE BOOK

The chapters in this book are self-standing. The content of this book is organized into two sections. The first section (Chapters I-VII) focuses on the technical aspects of dealing with the heightened need for security brought on by increasingly powerful information technologies. It discusses and presents models designed to address these pressing issues.

Section two (Chapters VIII-XV) attempts to define and describe ethics and social responsibility in the new age of information systems and takes the reader through some of the impacts these transforming technologies have on the characteristics and quality of institutions, on individuals, and society in general. Both sections contribute to the ongoing discussion so urgently needed for dealing with these complex phenomena.

A brief description of each chapter follows:

Section I: Information System Security

Chapter I titled, "Network Security Software," by Göran Pulkkis, Kaj J. Grahn, and Peik Åström of Arcada Polytechnic (Finland), provides a brief topical overview of state-of-the-art network security software and related skills and education needed by network users, IT professionals, and network security specialists. It presents a broad area of topics, such as protection against malicious programs, firewall software, cryptographic software, security administration software, security software development, network security software skill levels, and network security software skills in higher education.

Chapter II titled, "A Forensic Computing Perspective on the Need for Improved User Education for Information Systems Security Management" by Vlasti Broucek and Paul Turner of the University of Tasmania (Australia), identifies common security and privacy weaknesses that exist in e-mail and Web browsers, underlines some of the implications for organizational security, and tries to raise awareness amongst users. It recommends improved user training and education and concludes that IS security management can be achieved through a balanced and cooperative approach.

Chapter III titled, "Integrating Cooperative Engagement Capability into Network-Centric Information System Security" by Alexander D. Korzyk, Sr., of the University of Idaho (USA), suggests a departure from the traditional decentralized approach to security systems by adapting a system for industrial commercial organizations similar to the new concept of a Cooperative Engagement Capability used by the military to centralize the command over the entire suite of defensive assets.

Chapter IV titled, "A Methodology for Developing Trusted Information Systems: The Security Requirements Analysis Phase" by Maria Grazia Fugini and

Pierluigi Plebani of Politecnico di Milano (Italy), presents a methodology for designing security in advanced distributed Information Systems. It provides architecture for secure transmission of data among e-services and identifies the need for a plan of action in case of intrusion.

Chapter V titled, "A National Information Infrastructure Model for Information Warfare Defence" by Vernon Stagg and Matthew Warren of Deakin University (Australia), introduces an enhanced National Information Infrastructure model that provides greater defense against threats to information systems. The authors describe many threats that are not dealt with adequately in the current infrastructure and offer an enhanced model within the ICT sector.

Chapter VI titled, "Biometrics: Past, Present and Future" by Stewart T. Fleming of the University of Otago (New Zealand), aims to review the current state of the art of biometric systems. It conducts a detailed study of the available technology, examines end-user perceptions of such systems, and discusses a framework which is intended as a step towards providing more detailed guidelines to designers of interactive systems that incorporate biometric data. The importance of ethical and societal implications is mentioned.

Chapter VII titled, "User Types and Filter Effectiveness: A University Case Study" by Geoffrey Sandy and Paul Darbyshire of Victoria University (Australia), reports on Web-filtering software, in particular the filter squidGuard, used in a number of Australian universities. It describes three trials utilized to test its effectiveness and concludes that the ease by which the filter is bypassed points to the filter as superficial at best in trying to block against offensive material.

Section II: Ethics and Social Responsibility in the Information Age

Chapter VIII titled, "What is the Social Responsibility in the Information Age? Maximising Profits?" by Bernd Carsten Stahl of the University College Dublin (Ireland), argues that the idea of social responsibility is not a clearly defined concept and that it is essential to come to a concise definition to avoid confusion. The author then analyzes it and discusses its meaning in the information age. He hopes thereby to start a discussion with the purpose of rendering the term social responsibility useful.

Chapter IX titled, "The Social Contract Revised: Obligation and Responsibility in the Information Society" by Robert Joseph Skovira of Robert Morris University (USA), introduces the social contract as a basis for responsibility and obligation. It discusses the changes in this contract brought about through the Internet. It depicts three traditional social contracts — the Hobbesean, Lockean, and Rousseauean — and raises the question of what it means to take responsibility for one's behavior as an individual or corporation in the information society.

Chapter X titled, "The Influence of Socioeconomic Factors on Technological Change: The Case of High-Tech States in the U.S." by Rasool Azari and James Pick of the University of Redlands (USA), investigates the association of techno-

logical development with socioeconomic factors for 74 counties in 12 high-tech states in the United States. The findings are addressed relative to the research literature. Unequal access to technology, ethics, and social responsibility are discussed. Policy implications are examined.

Chapter XI titled, "Social Responsibility and the Transition Toward a Knowledge-Based Society in Latin America" by Heberto J. Ochoa-Morales of the University of New Mexico (USA), talks about the digital gap in the countries of South America and discusses the role of private and public institutions in closing the digital gap.

Chapter XII titled, "Information Systems Ethics in the USA and in the Arab World" by Husain Al-Lawatia and Thomas Hilton of Utah State University (USA), explores the similarities and differences between Arab and American students in information systems ethics through a survey on the use of personal computers at work. The findings point to interesting statistical differences in the average strength of several responses, but there is no disagreement as to the ethicality or non-ethicality of any survey item.

Chapter XIII titled, "Lemon Problems in the Internet Transactions and Relative Strategies" by Li Qi and Zhang Xianfeng of Xi'an Jiaotong University (China) discusses the information asymmetry which exists, not only in traditional business environments, but also in the Internet. This asymmetry encourages the sale of inferior products and services through Internet transactions. Some strategies are offered for avoiding or lessening the likelihood of these "lemon problems" to occur.

Chapter XIV titled, "Reputation, Reputation System and Reputation Distribution — An Exploratory Study in Online Consumer-to-Consumer Auctions" by Zhangxi Lin of Texas Tech University (USA), Dahui Li of the University of Minnesota Duluth (USA), and Wayne Huang of Ohio University (USA), explores the value of reputation in the area of e-commerce by evaluating data directly collected from eBay.com. Inherent problems of the existing reputation systems are pointed out. A stochastic process model is used to analyze the formation of the distribution.

Chapter XV titled, "Privacy Perspective from Utilitarianism and Metaphysical Theories" by Hasan A. Abbas and Salah M. Al-Fadhly of Kuwait University (Kuwait) talks about the concept of privacy in the information age and tries to present the topic from philosophical perspective.

REFERENCES

Chandler, A. (1991). *Scale and Scope.* Cambridge, MA: Harvard University Press.

Grupp, H. & Maital, S. (2001*). Managing New Product Development and Innovation: A Microeconomic Toolbox.* Cheltenham, UK: Edward Elger.

Johnson, D. (2001). *Computer Ethics (3rd Ed.).* Upper Saddle River, NJ: Prentice Hall.

Laudon C. K. & Laudon, J. P. (2002). *Management Information Systems: Managing the Digital Firm (7th Ed.).* Upper Saddle River, NJ: Prentice Hall.

OECD. (1998). *21st Century Technologies: Promises and Perils of a Dynamic Future.* City, County: OECD.

Schneier, B. (2000). *Secret and Lies: Digital Security in a Network World.* New York: Wiley Computer Publishing.

Rasool Azari
School of Business
University of Redlands, USA
February 2003

Acknowledgments

This book is the work of many people whose expertise and diligence contributed in numerous ways. I thank them all. I am deeply indebted to Mehdi Khosrow-Pour, a friend and the senior editor of Idea Group Publishing Inc. for introducing me to this timely and interesting project. My special thanks also go to other members at Idea Group Inc., especially Jan Travers and Amanda Appicello who organized and coordinated the process from its inception through its completion.

Furthermore, credit certainly is due to all the authors of the chapters for taking the time and energy to contribute to this book. In addition, my gratitude is extended to the blind reviewers who worked on the early drafts of these chapters and whose contribution cannot be measured easily. And I gladly credit my colleague, Professor James Pick, whose helpful insights and advice I have gratefully accepted many times. Finally I want to acknowledge my wife, Gabriele Azari, who keeps position with me on the home front throughout whatever weather is blowing our way. I thank her for her patience and encouragement.

Rasool Azari
School of Business
University of Redlands, USA
February 2003

Section I:

Information System Security

Chapter I

Network Security Software

Göran Pulkkis
Arcada Polytechnic, Finland

Kaj J. Grahn
Arcada Polytechnic, Finland

Peik Åström
Arcada Polytechnic, Finland

ABSTRACT

This chapter is a topical overview of network security software and related skills needed by network users, IT professionals, and network security specialists. Covered topics are protection against viruses and other malicious programs, firewall software, cryptographic software standards like IPSec and TLS/SSL, cryptographic network applications like Virtual Private Networks, secure Web, secure email, Secure Electronic Transaction, Secure Shell, secure network management, secure DNS and smartcard applications, as well as security administration software like intrusion detectors, port scanners, password crackers and management of network security software management. Tools and API's for security software development are presented. A four-level network security software skill taxonomy is proposed and implications of this taxonomy on network security education is outlined. University and polytechnic level network security education is surveyed and the need for inclusion of network security software development skills in such education is pointed out.

INTRODUCTION AND BACKGROUND

The steadily growing international computer network user community needs an expanding staff of well educated network security professionals to guarantee the reliability of the global IT infrastructure of computer nodes in wired and wireless networks. Network security tools are usually software tools. Network security professionals should know these tools, how to use and develop them, and know what kind of network security they can provide.

In accordance with Oppliger (1999, preface) we define network security as "a set of procedures, practices and technologies for protecting network servers, network users and their surrounding organizations." Network security software (computer programs) covers the area defined above. In order to give a more structured picture of network security software, the material has been organized into the following topics:

- Protection against malicious programs
- Firewall software
- Cryptographic software
- Security administration software
- Security software development
- Network security software skill levels
- Network security software skills in higher education

The text gives a topical overview of network security software: the topics are not covered in detail, and most topics are briefly introduced and left for further study. The main objective is to present "State-of-the-Art" of network security software and to discuss related skills and education needed by network users, IT professionals, and network security specialists.

PROTECTION AGAINST MALICIOUS PROGRAMS

Malicious software exploits vulnerabilities in computing systems. In Bowles and Pelaez (1992) is presented a taxonomy, in which malicious programs are divided into two categories:

1. *Host program needed*
   - **Trap door**

     A trap door is a secret entry point bypassing normal authentication procedures to a program. Trap doors have for many years been used legitimately in program development for debugging and testing purposes. Malicious use of trap doors is a serious security threat.