Enterprise Information Security and Privacy

Edited by C. Warren Axelrod, Jennifer Bayuk and Daniel Schutzer

Reviewed by Sarathy BSP Emani, CISA, CISM, the proprietor of MEQPRIMA Advisory Services (*www.meqprima.com*), a software process and quality improvement research organization. He has more than 25 years of related industry experience. He is a member of ISACA's Publications Subcommittee.

The IT industry has been witnessing an accelerated rate of security breaches in the rapidly expanding technologies. Yesterday's solutions may be stale or may act as guidelines. Today's solutions may be strategies only for survival. Solutions for tomorrow's unknown risks may be uncertain, but would need guidelines to ensure security and privacy to the best of abilities. This book serves as a reference for information security and privacy professionals.

The book takes the approach of examining and questioning the current and traditional approaches to determine their strengths and weaknesses and to suggest paths forward that will overcome their deficiencies.

To meet the objectives of this book, 19 authors were chosen who have strong practical backgrounds and who have succeeded in providing recommendations that are realistic, visionary and doable in the rapidly changing technical and social worlds.

Three editors contributed in two different ways. The editors have included their own comments in each chapter to stimulate thought and discussion. They encouraged authors' creative thinking and presentation based on their backgrounds—leading to certain differences in referencing formats, but with no significant impact on content.

This book is organized into three parts and contains 13 chapters, followed by an appendix. Every page has footnotes with references to chapters of books, articles of journals and web pages.

> "Solutions for tomorrow's unknown risks may be uncertain, but would need guidelines to ensure security and privacy to the best of abilities."

Part I, Trends, traces the history of security, privacy and information technology. It contains five chapters. Each chapter is organized by background, observations, recommendations and future trends. The chapters in this section address data classification and the relationship between security and privacy, data protection, and Payment Card Industry Data Security Standards; identify three categories of challenges and provide recommendations; and discuss the human factor with respect to protecting privacy and monitoring for fraudulent behavior.

Part II, Risks, tackles the relationships of information security risks with others. It contains four chapters.

Part III, Experience, covers a collection of experiences from different sectors. It contains four chapters, each covering one sector: financial services, energy, transportation and academia.

The appendix, Key Information Security Law References, covers US federal and state statutes and regulations, court decisions, and decrees; EU directives; and laws of other countries. This appendix can act as a quick reference.

In its entirety, the book instigates thoughts for future risk and security concerns.

EDITOR'S NOTE
Enterprise Information Security and Privacy is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this *Journal*, visit *www.isaca.org/bookstore*, e-mail *bookstore@isaca.org* or telephone +1.847.660.5650.