Foreword

The French statesman Georges Clemenceau once said that "warfare is too serious a matter to entrust to military men." Today, the same thing could be said about information warfare, which is fought every day over the Internet and on corporate networks. Indeed the permanent and global nature of security threats and the increasing complexity of IT infrastructures are leading organizations worldwide to revise their approach to information security. Hiring and entrusting the ICT equivalent of military men, i.e. security technologists and white-hat hackers, is no longer enough.

Most organizations fully recognize that they need to continuously improve their internal security culture, establishing and maintaining proper security governance processes. However, this is easier said than done. Some European companies still rely on obsolete security standards like the 17799, which were developed when current ICT threats and complexities were still unheard of. The more recent ISO/IEC 270001 standard has finally introduced a notion of security policy life-cycle; but in today's dynamic ICT environments, emerging threats and sudden technology changes may require much more agile decision-making procedures. For all these reasons, establishing a security governance process tailored to an organization's needs is still considered more an art than a science in most domains.

This book, written by internationally recognized leaders in this field, takes a significant step toward a scientifically sound, repeatable approach to information security governance. Its initial section takes a fresh look at existing security governance frameworks, challenging conventional wisdom on what information security actually is. Also, this section provides some sound advice on how to choose the right security governance framework and processes for a specific organization in critical domains like banking and healthcare. Another important contribution is providing a clear outline of the legal issues underlying corporate security governance, including the (law-mandated or contractual) responsibilities of the different organizational roles.

The second section of the book deals with enterprise-level security governance processes. It covers most standards for security governance at the enterprise level, highlighting their different models for decision-making, including risk-based ones. Describing some interesting case studies, this section leads the reader toward a dynamic, flexible security governance based on decentralized decision making, where security objectives and strategies are the main focus – without forgetting traditional security risks and controls.

The third section of the book looks at a number of open frontier issues that are likely to accompany information security and security governance into the 21st century. This fascinating set of research essays, each suitable for supporting a Ph.D. level short course, goes from the increasingly important role of biometrics to malware, risk monitoring, and ontology-based models.

As a whole, this book is a "must read" for both advanced practitioners and researchers working on security governance issues. From a researcher's point of view, the book chapters and their rich bibliography are ideal starting points for young scientists looking for a new topic, or for experienced researchers wishing to gain a good understanding of the state of the art in this field. However, this book will be even more useful to practitioners working toward establishing a sound security governance process in their organization. In order to improve security, organizations have to understand the different assumptions underlying the standards and the distinctive features of different decision-making procedures. The techniques discussed in the book are a key prerequisite to implement the "right" security governance practices, ensuring that crucial decisions about information security are taken in the best possible way.

Ernesto Damiani
University of Milan, Italy

Ernesto Damiani *is involved in several projects at different institutions. He is a Professor at the Dept. of Computer Technology, University of Milan, Italy. Since Jan 2008, he has been the Head of the University of Milan's Ph.D. School in Computer Science. He holds visiting positions at several other places, including: UTS: University of Technology, Sydney, Australia; eBMS, University of Lecce, Italy; Computer Science Dept, LaTrobe University, Melbourne, Australia; and Computer Science Dept, Free University of Bozen, Italy. He is a Senior Member of the IEEE, and a Distinguished Scientist/ Member of ACM.*