Many students and young professionals want to know which topics they should master in the information security field. The answer is contained in the two volumes of the Computer Security Handbook, which has 75 chapters, written by industry professionals. The sixth edition provides an update to the content of each chapter while maintaining the structure of the previous edition, which was released in 2009.

The book covers the 10 domains of the Common Body of Knowledge by the International Information Systems Security Certification Consortium, Inc., (ISC)². It is divided into eight parts, starting with the foundations of computer security and going from the typical security life cycle to the identification of preventive measures, which may be both technical and organizational. In case preventive measures have been bypassed or breached, readers can focus on the sections about detecting security breaches and preparing for response and remediation. The handbook also covers management’s role in security, public policy and other related considerations. Because of the way this book is written, understanding these topics requires minimal technical knowledge.

In the era of Wikipedia and Google, one might ask whether there is any need for reference work such as this book. Indeed, it is possible get an overview of most of the topics mentioned in this book, including biometric authentication or business continuity planning, just by surfing the Internet, but it might be a bit harder to find comprehensive articles on issues such as using social psychology to implement security policy or other complex topics covered by this book.

One shortcoming of this handbook is that it tends to focus primarily on US laws, regulations and standards (e.g., US legal and regulatory security issues, working with law enforcement). However, it does provide some coverage of the European legal framework. Another shortcoming is that for some topics, readers may need to jump from chapter to chapter to get a full understanding of the subject. This happens, for instance, with discussions on operating systems such as Microsoft Windows or Unix. To facilitate this process, readers can refer to the index at the end of volume 2.

In a business world where security professionals are required to master—in breadth and in depth—a wide range of security-related technologies, methodologies and techniques, having a sound and trustworthy point of reference to guide them through the variety of topics and expertise required is essential. Computer Security Handbook, with its more than 2,000 pages and abundance of referential material, is just the right book for the job.

EDITOR’S NOTE
Computer Security Handbook, 6th Edition is available from the ISACA® Bookstore. For information, visit www.isaca.org/bookstore, email bookstore@isaca.org or telephone +1.847.660.5650.

Reviewed by Dino Ippoliti, CISA, CISM, an expert consultant at inspearit. He has been a practitioner in information and computer security, IT system auditing, and software and system engineering process improvement for more than 17 years in multiple industries. Ippoliti is a member of the ISACA® Publications Subcommittee and a mentor in ISACA’s Pilot Mentoring Program.