Thomas J. Shaw, Esq., Editor. Information Security and Privacy: A Practical Guide for Global Executives, Lawyers, and Technologists. Chicago: American Bar Association, 2011, 395 pages.

Reviewed by *Philip A Houle*, Professor of Information Systems, College of Business and Public Administration, Drake University.

Subject Area: Information Systems

The editor argues in the forward of the book that in today's world of digital information and the potential chaos, it is imperative that there be a means of control to prevent loss or compromise to our data. The amount of information in digital format is exploding. The risks to organizations and individuals are dramatically increasing in terms of loss of privacy and exposure to financial loss. The editor has two primary audiences in mind: first are the top-level leaders in the organizations and second are the lawyers and technology experts who provide advice on how best to manage the issues.

This book is a product of the Information Security Committee of the American Bar Association's Science and Technology Section. It includes the collective contributions of more than sixty individuals across a variety of organizations all connected with the subject matter. However, the specific contributions any one of these individuals is not identified.

The stated goal is "to inform" and "to provide the tools to identify and manage the business, legal, and technical risks of protecting information on a global scale" (p. xiii).
Protecting information on a global scale is more important today with the exploding rise of e-commerce applications based on the Internet and the World-Wide-Web. Increasing numbers of organizations are moving into applications based on the Internet to sell their products and services. Applications commonly called Web 2 are becoming more prominent. Significant applications in this arena, such as YouTube and Facebook, have arrived within only the past decade; yet today dominate much of what individuals and organizations consider as they use the Internet. This book seemingly provides a basis for understanding how to implement methodologies to manage the risks and opportunities.

The book consists of eight chapters and four appendices. In addition to these, there is a listing of authorities (legal statues, rules, regulations and definitions) and a listing of court cases relevant to the presentation.

Each chapter has a summary box near the beginning of the chapter that contains approximately a half-dozen bullet points indicating issues addressed in the chapter that answers the question, "What Global Executives Need to Know." These points provide a nice summary of the contents of the chapters in terms of the intended audiences.

Chapter 1 (*Introduction to Information Security*) centers on defining the concepts in information systems and the resulting risks and issues with security and privacy. It introduces the concept of having a methodology that an organization can implement to manage the risks connected with security and privacy. The methodology is presented as the Information Security and Privacy Lifecycle. The lifecycle has five steps: Synthesis of requirements; analysis of exposures to legal liability; assessing risk; implementing controls; and compliance, audit and certification. The chapter also addresses the need to protect data, the definition of information security, and the relationship between information security and privacy. Basically, privacy requires that information be secure.

Chapter 2 (*Information Security and Privacy Laws and Regulations*) centers on domestic and international laws and regulations that deal with security and privacy and that must be considered when setting up policies and controls within the organization. It also looks at the issue of business continuity management practices.

Chapter 2 starts with a review of United States federal laws that managers must consider. These include the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, the Health Information Technology for Economic and Clinical Health Act, Sarbanes-Oxley, Federal Information Security Management Act, the Federal Information Security Management Act, the Federal Trade Commission Act, the Fair and Accurate Credit Transactions Act, the Computer Fraud and Abuse Act, the Digital Millennium Copyright Act, the Children's On-Line Privacy Protection Act, the Veteran's Affairs Information Security Act, the Federal Privacy Act, the Federal Rules of Civil Procedure, the Family Educational Rights and Privacy Act, the Communications Act, and Dodd-Frank Wall Street Reform and Consumer Protection Act. The size of this listing of these federal laws hints at the complexity faced by managers to properly comply. The chapter outlines the implications of each law and lists specific information about the details of the laws to the organization.

In addition to the federal laws, Chapter 2 presents information about United States state laws and international laws. The international law section includes many countries such as Canada, European countries, Latin America, as well as Asian/Pacific rim countries.

Chapter 3 (*Information Security and Privacy Liability*) looks at legal liability exposures relating to security and privacy. Liability claims can arise based on the laws and regulations outlined in Chapter 2. However, claims can also arise based on criminal statues and can be based on conduct involving contracts between parties, conduct involving torts, and actions related to consumer protection regulations.

Chapter 4 (*Information Risk Management*) examines how to reduce or minimize the legal and business risks in protecting information. It introduces the concept of information risk management (IRM). IRM is intended to reduce legal and business risks that arise when protecting information. It involves risk assessment and cost-benefit analysis of possible options to control risk.

Chapter 5 (*Information Security and Privacy Controls*) looks at the issue of controls to attain security and privacy. It starts with an analysis of controls mandated by laws and regulations. It then analyzes control issues required to maintain competitive advantages and to minimize legal risk. The chapter looks in depth at the issue of authentication (user identification) in the world of the public internet. This includes examining public key encryption infrastructures and the management of keys and of standards for their use. In addition, the chapter examines the threats to security and privacy that arise from personnel.

Chapter 6 (*Information Security and Privacy Best Practices*) introduces the idea of best practices and the need for managers to compare their organizational practices with best practices. Best practices come from a survey of what is being done across industries and especially in similar and competitive organizations. If there are differences, then there must be documents that outline these differences and that justify the differences in terms of effectiveness. The chapter also introduces the need for an organization to formally audit security and privacy plans and policies.

Chapter 7 (*New and Emerging Technologies*) examines the challenges that arise from new and emerging technologies. One of the newer forms today is social networking. Social networking has dramatically altered the way commerce works and the way individuals and organizations interact. This impacts employees in terms of their relationships with others inside the organization as well as beyond the organization. The need for policies and standards becomes apparent. Another newer technology is the use of cloud computing to host critical applications. These applications are moved to vendors in the Internet and the issues of policies to protect security and privacy must be expanded to include these new relationships.

Chapter 8 (*The Role of Advisors and Wrapping Up*) looks at the roles of the two primary advisory groups regarding information security and privacy: lawyers and information security technologists. It explores the typical roles played by each in relation to the business executives of the organization. It also explores how these roles must work together in devising organizational plans and policies.

As stated earlier, the book also includes four appendices. These appendices provide supporting and more detailed information connected with the presentation of the eight chapters. The appendices and titles are as follows:

- Appendix A (*Information Security and Privacy Standards and Guidelines*).
- Appendix B (*Glossary of Terms, References, and Industry Standards*).
- Appendix C (*United States State Information Security and Privacy Laws*).
- Appendix D (*Best Practice Example Documents*).

As I read this book, I was very impressed with the complexities of information security and privacy issues. This is a statement from an academic who has worked with technology for almost fifty years and who routinely teaches undergraduate and graduate courses that address these same issues. The book impacted my understanding of the issues and should do the same for any executive who chooses to read the book. I wouldn't expect every reader to absorb and to understand all of the legal and technical details. However, I would expect every reader to appreciate the fact that he or she must engage both lawyers and technology experts to insure that the organization is a good custodian of information security and privacy