Preface

Organizations of all types and sizes around the world rely heavily on technologies of electronic commerce (e-commerce) for conducting their day-to-day business transactions. Obviously these technologies and all information assets that they process should be protected against fraud, theft and misuse both from internal and external threats. Providing organizations with a secure e-commerce environment is a major issue and challenging one in today’s Digital Economy. Without total secure e-commerce, it is almost impossible to take advantage of the opportunities offered by e-commerce technologies. Furthermore, without secure e-commerce applications and practices, it is very difficult to gain the confidence and trust of the consumers and clients in using this technology. Security architecture must be designed to protect organization’s e-commerce operations from both known international and external threat, and must be flexible enough to stop less-defined and projected threats. One important element of e-commerce security is top management understanding of the significant importance of the issue and of the commitment given to develop and operate a totally secure e-commerce environment.

*e-Commerce Security: Advice from Experts* covers a wide range of existing e-commerce security issues and challenges, and offers many solutions for managing security risks. Experts in the field of e-commerce and e-commerce security offer insight to key issues of current e-commerce
security and future challenges facing e-commerce professionals in maintaining a secure e-commerce environment. The following paragraph describes the essence of the chapters in this book.

Chapter Summaries

Chapter I, *An Overview*, by Mehdi Khosrow-Pour of the Information Resources Management Association, is an introduction to the topic of e-commerce security. Khosrow-Pour discusses the benefits of e-commerce including online transactions and the sharing of valuable information. The chapter also discusses the risks of e-commerce and the need for a security infrastructure to prevent damages caused by criminal activity. By using a Total E-Commerce Security Program, businesses can protect themselves from dilemmas such as the theft of essential client and business information. Khosrow-Pour outlines what is entailed in building and maintaining a secure e-commerce environment.

Chapter II, *Learning from Practice*, consists of interviews conducted with eight leading e-commerce security experts around the world. In this chapter, they share their experiences and knowledge in the field of e-commerce security. Topics discussed include secure payments, interoperability, consumer/client protection and future challenges facing e-commerce professionals.

In Chapter III, *How One Niche Player in the Internet Security Field Fulfills an Important Role*, Troy Strader, Daniel Norris and Philip Houle, all from Drake University, and Charles Shrader from Iowa State University, examine the efforts of Palisade Systems to improve the potential of their products in the changing e-commerce environment. Issues faced by Palisade Systems include taking advantage of recent legislation passed regarding privacy on the Internet, the growing need for security on the
Chapter IV, *Personal Information Privacy and EC: A Security Conundrum*? by Edward Szewczak of Canisius College in Buffalo, covers the issues of personal information privacy (PIP) and e-commerce. The main focus of this chapter is privacy and barriers in the enforcement of privacy protection. Szewczak’s chapter discusses how Internet users are monitored without their consent and how this information could possibly be misused.

Chapter V, by Michelle Fong of Victoria University, is titled, *Developing Secure E-Commerce in China*. China is known for using e-commerce as a growth and modernization in their country. This chapter looks at why business-to-consumer (B2C) online transactions are low. For example, the chapter shows that there are inconvenient and insecure forms of electronic payment. In order for e-commerce to grow, security must improve and earn the trust of the user. Fong’s chapter discusses solutions and recommendations for this problem.

Chapter VI, *Identifying and Managing New Forms of Commerce Risk and Security*, by Dieter Fink of the Edith Cowan University in Australia, focuses on Risk and Security Management (RSM). Fink discusses the risks of unprotected e-commerce systems and what solutions offer protection from these risks. Some solutions include firewalls, digital signatures and encryption. The chapter covers new forms of risk and security that are dangers to a system. The chapter shows how to make an effective RMS approach to an e-commerce system.

Chapter VII, *E-Commerce Security and the Law*, by Assafa Endeshaw of the Nanyang Business School in Singapore, emphasizes the need for a secure network. This chapter explains why it is essential to have clear, easy-to-implement regulations and policies. In order to provide a secure e-commerce environment and gain trust of users, organizations and legal departments must get involved. The chapter discusses various laws that have been created to protect a user from identity theft, how offices have
been created to investigate and prevent hacking, and talks about the crackdown of unauthorized use of intellectual property. The chapter concludes with solutions and recommendations to the problems discussed.

Chapter VIII, *Rethinking E-Commerce Security in the Digital Economy: A Pragmatic and Strategic Perspective*, by Mahesh Raisinghani of the University of Dallas, discusses the importance of management understanding of advanced technology. Knowledge of advanced technological systems assists in creating more robust, scalable and adaptable information systems for the organization dedicated to continuous improvement and innovation. The key questions covered in this chapter include assessing status quo and modus operandi. Raisinghani proposes alternative solutions and recommendations for the future of the digital economy.

Chapter IX, *Security and the Importance of Trust in the Australian Automotive Industry*, by Pauline Ratnasingam of Central Missouri State University, focuses on the Australian Automotive Industry and security issues in technical, political and behavioral perspectives. The chapter discusses the importance of trust, how to gain trust and how to establish dependable business relationships as a means to mitigate risks in EDI in the Australian automotive industry.

Chapter X, by Daniel Ruggles from Consulting Associates, LLC, is titled *E-Commerce Security Planning*. In this chapter, Ruggles discusses the importance of establishing an e-commerce trust infrastructure that will protect three major areas of an e-commerce site: the internal network, the perimeter network access and the external network. The chapter discusses how to build an e-commerce trust infrastructure and how to create a balance between functionality and accessibility with an e-commerce system.

As emerging e-commerce technologies offer new opportunities to organizations all over the world to conduct business in ways that until several years ago was considered unthinkable, it is extremely important to
protect both the organization and its clients from fraudulent acts and misuse of these technologies and information that they process. Without a totally secure e-commerce environment, all efforts to obtain the trust and confidence of the user communities will be thrown to the waste and will not bear any meaningful results. Planning and conducting totally secure e-commerce should be the first step in developing any kind of e-commerce applications. For those organizations that have already been involved in using e-commerce security, they should continuously reassess their e-commerce security and to make sure that all vulnerabilities are planned for and possible threats are also planned for. Achieving a totally secure e-commerce environment begins with a well-informed management about the significance of secure e-commerce. I hope that the knowledge and advice provided in this book can become instrumental in understanding many issues, including those of e-commerce security, and can provide insights and ideas that can be utilized in support of e-commerce security. As always, your valuable comments and feedback will be greatly appreciated.

Mehdi Khosrow-Pour, D.B.A.
Executive Director and President
Information Resources Management Association, USA