Preface

In the 2003 publication, *The National Strategy to Secure Cyberspace*, the United States Government acknowledged, "our economy and national security is now fully dependent on information technology and the information infrastructure" (U. S. Government, 2003, p. 9). The candid use of the word "fully" is no overstatement. If the Internet infrastructure were significantly compromised, critical systems supporting supply chains, financial markets and telecommunications, for example, could simultaneously be severely handicapped or completely cease from functioning.

Particularly since the turn of the century, modern society's dependence on cyber and information related technologies for daily living has increased at an astonishing rate. Entire cultures of what many call 'developed nations' such as the United States are engulfed in a cyber technology way of life that takes for granted the availability and integrity of information systems and the Internet. Additionally, in some "developing" nations, the outsourcing of knowledge work from developed nations has created high-technology subcultures in the developing world. While a global digital divide certainly exists between nations with ready access to cyberspace and those without such access, overall, an increasing global economic dependency on cyberspace is undeniable. Some argue, such as James Lewis in testimony to the U. S. Congress, "Cyber security is now one of the most important national security challenges facing the U. S. This is not some hypothetical catastrophe. We are under attack and taking damage." Indeed, the cyber security situation facing the U. S. has gotten worse in the past decade, while cyberspace now supplies the foundation of much of the nation's economic activity (Lewis, 2008).

This book addresses the growing societal dependence on information technologies by providing a literature resource for academics and practitioners alike that speaks to the pressing issues facing cyber security from both national and global perspectives. Book chapters cover critical topics to include information security standards, information overload, cyber privacy issues, information terrorism, the cyber security black market, threat assessment for enterprise networks, an analysis of critical transportation infrastructures with cyberspace implications, information sharing during catastrophic events, as well as chapters discussing trusted computing, honeypots and server hardening. The underlying premise of the book stresses the global nature of cyber security problems; in doing so, each chapter provides an analysis of specific threats facing society with proposed solutions. Ultimately, we hope this book will facilitate international cooperation to help build a more secure future in cyberspace.

Before continuing, it is worthwhile to review the term *security* and offer a formal definition to help explain why books such as this are valuable. Security is the condition of being protected, which includes freedom from apprehension and the confidence of safety; hence, assurance. We can think of security as that which makes safe or protects (Webster's Revised Unabridged Dictionary, 2008). Regarding information or cyber security, both practitioners and academics often stress the importance of three desirable aspects of security: Confidentially, Integrity and Availability. This CIA triad serves as a limited, but useful framework for thinking about and understanding security and how data and cyber-based systems need protecting (Whitman & Mattord, 2004). Security becomes especially critical in hazardous environments when the risk of danger and the consequence from damaging incidents are high. This is the reason why cyber security has become so critical in recent times. We have become progressively dependent on cyberspace for daily living yet the cyber environment is full of serious dangers.

Now that we have briefly framed the term security, we may ask, what aspect of security is most important to enhance our understanding and lower risks? In his edited book titled, *Information Security Management: Global Challenges in New Millennium*, Dhillon argues that the management of information security should be broader in scope than just focusing on the technological means to achieve proper security (2001). This indeed is the case with the current text: fully grasping today's challenges requires a broad view of cyber security that includes both technical and managerial dimensions. To this end, each chapter offers a valuable perspective of cyber security and information assurance. If read from cover to cover, the reader will gain a holistic understanding and systems view of cyber security challenges. While the book is not encyclopedic in scope, it offers a broad view of security challenges through 18 chapters, each dedicated to a different but important topic in the cyber security domain. Each chapter was double blind reviewed. Authors went through a process of submitting a proposal, completing a manuscript, and then revising the manuscript while responding to comments from at least three external reviewers. Finally, each author of an accepted manuscript worked with me to produce a publishable chapter. This process has been immensely valuable to me as the editor. I thoroughly enjoyed working with each author and found the publication process to be professionally satisfying. In reviewing each chapter as the editor, I found myself enlightened and better educated about this dynamic, complex and critical field. It is my hope that readers will share a similar experience.

I divided the book into four major sections, each containing at least three chapters. Together, the four sections present a broad and global picture of major cyber security challenges. The first section offers chapters on the theme of *Risk and Threat Assessment*. The second section focuses on *Organizational and Human Security*. The third presents topics covering *Emergency Response Planning*. Finally, the fourth section covers important *Security Technologies*.

The book begins with a section on *Risk and Threat Assessment*. I placed this section first because of my belief that understanding risk and the threat environment is a foremost step in addressing security. In Chapter I, Jaziar Radianti and Jose J. Gonzalez discuss their observations of the black market for software vulnerabilities and the factors affecting its spread. They illustrate a system dynamic model and suggest that, without interventions, the number and size of black markets will likely increase. In Chapter II, Somak Bhattacharya, Samresh Malhotra, and S. K. Ghosh provide an attack graph approach to network threat identification. The chapter deals with identifying probable attack graph and risk mitigation in order to improve enterprise security. Chapter III introduces the insider threat and methods for preventing, detecting, and responding to this threat. In their work, Robert F. Mills, Gilbert L. Peterson, and Michael R. Grimaila define the insider threat and offer best practices for mitigating this serious problem. Chapter IV describes a method for assessing security infrastructure effectiveness utilizing formal mathematical models. Here, Richard T. Gordon and Allison S. Gehrke discuss a novel security measure that organizations can use to evaluate the strength of their security infrastructure. In the final chapter of this section, Chapter V, Ken Webb argues that a heightened risk for management has emerged from a new security environment that is producing asymmetric forms of information warfare. This chapter aims to provide guidance for future thinking to inform readers about information terrorism and the security implications for management.

The second section covers the important area of *Organizational and Human Security*. While sometimes described as the “soft” or non-technical side of security, this area is often at the very core of many security problems and incidents. In Chapter VI, Yves Barlette and Vladislav V. Fomin discuss major management standards, particularly ISO/IEC 27001 and 27002. Based on the findings of their literature review, the authors recommend how to successfully implement and diffuse information security standards in organizations. Chapter VII covers the important topic of information overload. Peter R. Marksteiner uses military doctrine to underscore the seriousness of the overload threat. The chapter provides a detailed discussion explaining the problem and suggests improvements concerning organizational communication effectiveness. In Chapter VIII, John W. Bagby posits that personally identifiable information flows along an “information supply chain” and offers a useful conceptual framework for balancing privacy and security. In Chapter IX, Indira R. Guzman, Kathryn Stam, Shaveta Hans, and Carole Angolano focus on the role of information security professionals in organizations. They explicitly focus on the specific roles, expectations and skills required by IT security professionals based in part on interviews conducted with security professionals. In Chapter X, the authors Nikolaos Bekatoros, Jack L. Koons III, and Mark E. Nissen discuss improving the structural fit of organizations involved in computer network operations (CNO). The authors use contingency theory research to inform leaders and policy makers on how to bring CNO organizations into a better fit in order to improve organizational performance. In Chapter XI, Rodger Jamieson, Stephen Smith, Greg Stephens, and Donald Winchester offer a strategy for government and a useful framework for identify fraud management. The authors based this framework on a literature review of related fields and organized the framework into anticipatory, reactionary and remediation phases.

The third section of the book deals with the emerging area of *Emergency Response Planning*. In light of serious external threats from terrorism and natural disasters, organizations must ensure that proper planning occurs to ensure continuity in the event of a disaster. In Chapter XII, Alanah Davis, Gert-Jan de Vreede, and Leah R. Pietron present a repeatable collaboration process as an approach for developing an incident response plan for organizations. The authors use collaboration engineering principles and present a process that consists of codified facilitation practices that can be transferred to and adopted by security managers in various types of organizations. Next, Chapter XIII deals with the possibility of a pandemic influenza, worker absenteeism and its impacts on the critical infrastructure of freight transportation as an illustration of how other infrastructures can be impacted. In this work, Dean A. Jones, Linda K. Nozick, Mark A. Turnquist, and William J. Sawaya then address the relevant question of how does this idea extend to other infrastructures, particularly those that are more information-oriented and less labor-intensive than transportation. Chapter XIV focuses on information sharing and information attributes within a disaster context. The authors Preeti Singh, Pranav Singh, Insu Park, JinKyu Lee, and H. Raghav Rao use content analysis to develop a prioritization framework for different disaster response activities. In Chapter XV, Gregory B. White and Mark L. Huson develop the community cyber security maturity model to provide a framework for states and communities to help prepare, prevent, detect, respond, and recover from potential cyber attacks. This model has broad applicability and can be adapted to nations and communities.

The fourth and final section offers chapters focusing on three vital security-related technologies. In Chapter XVI, Doug White and Alan Rea present essential server security components and develop a set of logical steps to build hardened servers. This chapter presents a complete model that includes advice on tools, tactics, and techniques that system administrators can use to harden a server against compromise and attack. In Chapter XVII, Jeff Teo provides an overview and direction of trusted computing and the goals of the Trusted Computing Group. This group uses trusted hardware in conjunction with enhanced software to provide better protection against cyber attacks. Chapter XVIII, the final chapter of the book, comes from Miguel Jose Hernandez y Lopez and Carlos Francisco Lerma Resendez. They discuss the basic aspects of Honeypots and how they are implemented in modern computer networks. The authors provide readers with the most important points regarding the characteristics of Honeypots and Honeynets, which are highly useful platforms in supporting security education and forensics.

It is my hope that after reading this book in part or in its entirety, readers will feel more knowledgeable and enlightened about the scope of challenges facing global cyber security. Considering the types of cyber threats facing our world, books such as this can make an important contribution by enhancing our understanding concerning the problems we are facing and solutions we should contemplate. I would enjoy hearing from readers about your opinions and experiences with this book. Feel free to contact me at knappkj@gmail.com.

With warm regards,
Kenneth J. Knapp, Editor
United States Air Force Academy, Colorado
November 2008

DISCLAIMER

Opinions, conclusions and recommendations expressed or implied within this book are solely those of the authors and do not necessarily represent the views of US Air Force Academy, USAF, the DoD or any other U. S. government agency.

REFERENCES

Dhillon, G. (2001). *Information Security Management: Global Challenges in the New Millennium*. Hershey, PA: Idea Group Publishing.

Lewis, J. A. (2008). *Cybersecurity Recommendations for the Next Administration Testimony by James A. Lewis, Center for Strategic and International Studies, September 16, 2008*. Washington D.C.: Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology.

security. (n.d.). *Webster's Revised Unabridged Dictionary*. Retrieved September 17, 2008, from Dictionary.com website: http://dictionary.reference.com/browse/security

U. S. Government. (2003, February). *National Strategy to Secure Cyberspace*. Retrieved May, 2004, from http://www.whitehouse.gov/pcipb

Whitman, M. E., & Mattord, H. J. (2004). *Management of Information Security*. Cambridge, MA: Course Technology - Thompson Learning.