BOOK REVIEWS

Gary C. Kessler
Editor
Gary Kessler Associates
Burlington, VT 05401
gck@garykessler.net

BOOK REVIEW

Knapp, K.J. (Ed.) (2009). *Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions*. Hershey, NY: Information Science Reference. 434 + xxii pages, ISBN: 978-1-60566-326-5, US$195.

Reviewed by Gary C. Kessler (gck@garykessler.net)

I freely admit that this book was sent to me by the publisher for the expressed purpose of my writing a review and that I know several of the chapter authors. With that disclosure out of the way, let me say that the book is well worth the review (and I get to keep my review copy).

The preface to the book cites the 2003 publication of The National Strategy to Secure Cyberspace by the White House, and the acknowledgement by the U.S. government that our economy and national security were fully dependent upon computers, networks, and the telecommunications infrastructure. This may have come as news to the general population but it was a long overdue public statement to those of us in the industry. The FBI's InfraGard program and the formation of the National Infrastructure Protection Center (NIPC) pre-dated this report by at least a half-dozen years, so the report was hardly earth shattering. And the fact that the bulk of the telecom infrastructure is owned by the private sector is a less advertized fact. Nonetheless, reminding the community of these facts is always a Good Thing and provides the raison d'être of this book.

The book is divided into four sections (18 chapters) that offer a nice flow in discussing the broad topic of information assurance (IA). It's important to note up front that this is not a general IA textbook but contains 18 very specific treatises.

Section I, titled "Risk and Threat Assessment," contains five chapters that lay the groundwork for understanding the concerns of the information security community to our information assets and resources. The first chapter describes the very interesting topic of the underground black market for the exchange of lists of software vulnerabilities and tools with which to exploit those vulnerabilities. The next chapter describes an automated approach to identifying threats to enterprise networks using attack graphs. The following

chapter discusses prevention, detection, and mitigation of insider threats, which is possibly the largest information security danger that we face. This is followed by a chapter about a mathematical model for assessing the efficacy of an organization's infosec infrastructure. The last chapter of this section discusses the impact of information terrorism and the asymmetric nature of Information Warfare. This section of the book, even alone, would grab a reader's attention to the problems at hand.

Section II is titled "Organizational and Human Security." Here, the book continues with six chapters describing the source of most of the major infosec weaknesses and problems, namely, people and organizational structures that often stand in the way of identifying and fixing problems. This section starts with a chapter about international standards for information security and a review of the literature that helps to explain the low level of adoption of these standards. The second chapter is the wonderfully titled "Data Smog, Techno Creep and the Hobbling of the Cognitive Dimension," describing new approaches to focus on the important, relevant data for decision-making and understanding in this era of an over-abundance of information that can literally over-stimulate us into inaction. This is followed by a chapter about striking a balance between privacy and security when developing public policies with respect to information. The following discussion explores the role of infosec professionals within an organization, and the tension between functionality and security when developing organizational policies with respect to information. Recognizing the increased reliance on computer networks in military applications, the next chapter describes Contingency Theory as a mechanism to guide the design and development of organizational structures that can improve the performance of information technology departments. The final chapter addresses methods with which to manage identity fraud.

Section III comprises four chapters and is titled "Emergency Response Planning." All too often, infosec policies focus on a single organization's plan to respond to a direct attack of some sort. The first chapter in this section discusses an information response plan designed using the principles of Collaborative Engineering, allowing a coordinate incident response plan across organizational boundaries within and between companies. The next chapter addresses threats to critical infrastructures due to worker absenteeism as a result of a pandemic (e.g., what would have happened if the H1N1 virus had continued to grow unabated, causing massive organizational shutdowns?). This is followed by a discussion of the importance of continued information system operations in order to maintain information sharing that is so critical during major catastrophes. The final chapter describes a Community Cyber Security Maturity Model, a framework so that states and local communities can build a cyber attack response policy that does not rely solely on a national response.

"Security Technologies" is the title of the final three chapters comprising Section IV. This section covers some of the more "traditional" aspects of infosec. The first chapter describes the development of a model for hardening both UNIX/Linux and Windows servers. The next chapter discusses the evolution of trusted computing with a focus on the role that the Trusted Computing Group (TCG) and trusted platform module (TPM) will play in increasing trust and information security in the global network society. The final chapter provides a detailed discussion of honeypots, including the purposes and implementations.

This book is far from a traditional information security textbook or professional reference -- no papers here, for example, on the mindset of the hacker, the role of intrusion detection systems, or information security issues related to current and future operating systems. That said, the book does cover some interesting and timely topics related to information security, and all are worthy of examination.

The book has several great qualities. First, it contains an excellent set of papers that are well written, current, and accurate. Second, the authors are from all over the world and the book, therefore, truly has a global point of view. From a format perspective, the compilation of each chapters' reference list into a single bibliography at the end of the book is a great touch and extraordinarily useful, and the index is outstanding.

The major downside of the book is its price. Even though the street price appears to be about 25% less than the retail price, it is a very costly book even for a text or professional reference. That said, it would make a good addition to a department or institutional library.

In today's environment with amazing availability of quality, peer-reviewed online resource, it is increasingly difficult to make the financial case for compendiums such as this volume. Part of the value of this book is, in fact, the topics that were selected. An individual might be hard-pressed to justify the expense but as a shared resource, this book has many compelling papers on topics to which infosec professionals should be paying attention.