

Title: Social and Human Elements of Information Security

Author: Manish Gupta & Raj Sharman

BOK Areas: Systems architecture, requirements engineering, risk management

Imagine my surprise when I saw that this book is actually a collection of essays written by a wide variety of people. This book brings together articles from researchers and practitioners in the financial, legal, technology, information security fields through original papers on all aspects of roles and effects of human and social dimensions of information security. As stated in the Preface, the key objective of this book is to “fill the gap in existing literature on human and social dimensions of information security by providing the readers one comprehensive source of latest trends, issues and research in the field.”

Each paper constitutes a chapter within the section. As a result the same or similar concepts are presented with different perspectives. I find this very enlightening. The papers are arranged in sections with each section containing 5 or more papers authored by persons representing academics and practitioners from the international community. The common thread through each section concerns the human element.

Section I: Human and Psychological Aspects – This section begins with the notion of humans and their frailties as related to the security practices for individuals, businesses, and organizations. It continues with the impact of humans on information security and why humans make poor security decision. The last paper in this section describes the incompatibility of software quality assurance procedures with the use of automatically generated code.

Section II: Social and Cultural Aspects – Beginning with a description of the complex nature of information security culture in a networked environment and a paper that examines the knowledge that might be available if both technology and human activity were seen as being equally important, this section brings together diverse elements of discourse. These papers are followed by a paper discussing social engineering as a technique for compromising information systems. The final paper in this section describes a model of a social paradigm for security and software engineering.

Section III: Usability Issues – The difficulty of using security configuration interfaces and how those interfaces can be improved is the subject of this first paper. It is followed by a paper describing the need for and the challenges of security usability and a paper describing the need and techniques for distinguishing between humans and automated computer programs on the Internet. One of these techniques is the use of CAPTCHAs. The last paper argues that it is possible to find a good compromise between quality of predictions and protection of personal data.

Section IV: Organizational Aspects – This final section begins with a paper describing the incorporation of human and social factors in the threat-vulnerability model of risks and the management of

vulnerabilities. Following this are papers addressing workplace monitoring and its implication for privacy concerns and aligning risk management with business requirements as a strategy for developing effective enterprise information security management. The ending papers highlight the issues resulting from the coalescence of system requirements elicitation, information security, and human factors and then the management of information as a critical corporate asset.

In addition to a detailed Table of Contents providing an overview of each chapter within each section of the book, the authors have included a Forward that lays the foundation for this book and its very contemporary and relevant papers. The theme is that although many organizations are relying purely upon technical solutions to implement their security policies this is an inadequate solution. The authors believe that it is a lack of understanding that prevents them from addressing security from the people, processes, and technology standpoints to implement a successful security strategy. This book is an attempt to close the information gap between technology and human factors.

By providing high quality research papers and industrial and practice articles on social and human aspects of securing information systems and infrastructure from social engineering attacks and real-world implications and implementations (practice) of the research the authors achieve their objective.