Foreword

The importance of security management in the development and operation of information systems (IS) has been growing with the ubiquity of information system use. Along with this growth and technological advances IS security has changed tremendously over the past decades and so have its scope, complexity, and the variety of analyzed security aspects. To meet these challenges IS security methodologies should become more industry specific and at the same time integrate organizational and technical aspects.

Securing the privacy of health information on systems is a major challenge to the widespread adoption of new healthcare information systems like the forthcoming German electronic health information infrastructure. Encouraged by the lack of healthcare IS research with respect to security, this work presents the design and development of an IS security methodology for the organizational and technical analysis of security issues in health care. Grounded on the research literature on IS security and healthcare IS, and a variety of current theories in the fields of information systems, business administration, and computer science, it develops a security analysis method for healthcare information systems. This security analysis method builds the foundation to practically examine the current status of the German healthcare telematics, its constitutive elements, and process management in order to identify possible vulnerabilities. Based on these insights, the work proposes appropriate solution mechanisms for the security management of the German healthcare telematics including recommendations for future IS developments in the health care sector.

Ali Sunyaev‘s work shows that IS security should be linked to the needs of an application area, both on the organizational and technical side. He clearly depicts the current security situation of German health information infrastructure and so facilitates a broader understanding of analyzing healthcare IS security. This work is an important contribution to the research field of managing information systems. In a methodological way it gives valuable impulses for combining different security approaches and research methods depending on the context of a security arrangement. The work appeals by its broad scope of theory, method engineering background, and its comprehensive argumentation. Researchers of information systems will gain new insights on which practical security analysis methods and theories are applicable given for healthcare information systems. For practitioners, it provides recommendations for orchestrating the development of secure healthcare IS and presents the identification of security problems in the current concept of German healthcare telematics.

I recommend this book as a valuable reading and resource. It provides new and promising insights into an IS security research field and inspires different kinds of readers to adopt a new perspective on healthcare information systems.

I hope this work will find the broad dissemination and attention it deserves.

Prof. Dr. Helmut Krcmar