Foreword

I am pleased to write the foreword to this handbook of research in the area of information security, as its objectives and content provide valuable insights into various aspects of human, social, and organizational issues in information security. The topics covered in the book range from privacy to social engineering, to enterprise security management to security awareness, and address very timely and important issues in the area of information security. The book presents an excellent product of both the academic and the practical knowledge of the authors that will assist researchers and practitioners in gaining significant knowledge on various topics in the field of social and organizational issues in information security.

It is commonly acknowledged that that a large proportion of the breaches to information systems security are made by insiders such as employees, contractors, and partners. High incident rates of security breaches by employees of an organization can be, to a large extent, explained by the fact that internal threats and vulnerabilities to information security are not adequately managed. With more than 15 years of experience in information security related positions, I believe that the organizational efforts to manage information security are typically focused on vulnerabilities in technological assets such as hardware, software, and networking, while laying little emphasis on managing other organizational resources such as such as people, policies, processes, and culture. In addition to lack of focus on non-technological aspects of an organization, technology-focused security countermeasures and protection mechanisms are usually centered on external threats, such as hackers and viruses while leaving organizations open to breaches from the inside.

It is to be understood that that organizational security safeguards cannot be achieved by technology alone. There is a significant aspect of protection that ties with the attitudes, awareness, behavior, and culture of the people involved. Understanding and incorporating social and organizational aspects can potentially represent a vital component of any information security program towards achieving security. Proper attention and support for the human, social, and organizational factors should therefore be seen as a vital element of a successful security strategy. The overall information security program of any organization can be vastly strengthened if greater emphasis is placed on internal threats to information security as insiders handle information and systems in their daily activities. In particular, social and organizational aspects of information security are under represented in academic literature, organizational practices, and in security strategies. One important aspect of managing organizational information security is security awareness and training to all the stakeholders of organizational performance. People from all levels of an organization need to understand security concepts, how the issues may apply to them, and how to use the organizational resources to protect information. One important aspect of this handbook is that is has a few chapters on security awareness that provides excellent overview of challenges and solutions for threats arising from lack of security awareness in employees. In addition, the technology itself can make a contribution by reducing the demands upon users, simplifying protection measures, and automating a variety of safeguards.

When Manish approached me to write the foreword of this book, I was delighted at the prospect. I am pleased to be able to recommend this book to readers, be they those looking for substantive material on information security or looking to understand an important aspect of social and organizational liabilities in information security. The chapters in the book raise and discuss a number of pressing issues that organizations are facing today, and also offers an overview of potential solutions. The primary benefit of the book is in showing that successful security strategies rely on well-thought out and executed organizational processes, based not just upon information technology hardware and software products but also on social, cultural, and organizational aspects. The book provides both an initial step towards better understanding the process and peoples' aspects of managing information security and a detailed discourse on embarking on a continuous improvement of the security program.

John C. Walp Jr.
Corporate Information Security Officer
M&T Bank Corporation, Buffalo, NY