During the past two decades, the Internet has evolved from a technologically sophisticated tool to a commonly used and accepted medium for communication. The promise of interconnectedness has been realized, providing unprecedented access to people and information. Despite its promising and meteoric rise to prominence, Internet technology also presents great challenges. The open nature of the Internet is highly insecure, leading to new questions about the security and quality of information. Moreover, the promise of interconnected access raises the potential for new threats, causing us to rethink the meaning and value of privacy in this environment. Individuals and organizations are potentially endangered in new ways by threats that may emanate from both internal and external environments.

Information security encompasses a broad range of topics and forms. It is, nonetheless, defined by the common aim of preserving the integrity, availability, and confidentiality of information system resources. With the introduction of information technology and the resulting security challenges that organizations face daily, it has become essential to ensure the security of the organization's information and other valuable assets.

Enterprises facing security threats demand powerful and flexible approaches that can match the dynamic environment in which these threats emerge. Challenges related to telecommunications and data security within the computer and transmission network include threats from online fraud, identity theft, illegal content, hacking, and piracy, to name a few. Security breaches such as distributed denial-of-service attacks and virus infections have highlighted the vulnerability of the information systems as end-users become more dependent on these systems. Complicating the issue is the fact that computer attacks can access personal information, raising both privacy and economic costs for individuals and organizations. Such costs can be expected to escalate as data generation and reliance by individuals and organizations increase on a daily basis.

Many organisations beginning to advocate security policies are relying purely upon technical solutions. However, information security is only partly about technology. A lack of understanding persists about the strategic importance of managing information security and the need to address security from a people, processes, and technology standpoint in order to implement a successful security strategy. Information security is not a problem which needs to be solved, but a process to be managed proactively. This process does not only require safeguarding information from the development and design stage of the new systems to their implementation, but it also requires a more holistic emphasis that goes beyond technology to address the social and human dimensions of communications, psychology, marketing, and behavioural change.

This holistic approach encompasses technical and procedural controls involving technology and human factors—the people who purchase, implement, use, and manage that technology. The human element can become the leaky faucet that spills sensitive information, as employees are often the weak-
est link when it comes to information security. People who manage and implement information security strategies must take this reality into account as they respond to vulnerabilities that ultimately impact the effectiveness of the organisation.

This book attempts to close this gap between technology and human factors by exploring the development and implementation of information security strategies. Information security is not merely a technological issue—it is also a human issue. As such, it invokes all of the complexity, unpredictability, and wonder that human beings bring to their creative enterprises.

Sylvia Kierkegaard
President
International Association of IT Lawyers (IAITL)

Sylvia Mercado Kierkegaard (BA, MA, MSc International Business and Law Summa cum laude, PG Dipl. Law, LLM, PG Dipl. EU Law, PhD) is the author of over 2000 publications. She is the editor-in-chief of the Journal of International Commercial Law (DOAJ-access), International Journal of Private Law (Inderscience) and associate editor and editorial board member of over 20 international journals, including the Computer Law and Security Report (Oxford-Elsevier), where her articles regularly appear. She is the president of the International Association of IT Lawyers (IAITL) and chairs numerous international conferences dealing with information technology and law. She is also the EU senior legal expert on information security for the EU-China Info Society project. Her international experience includes working in Europe, the Middle East, North America, and Asia advising clients on a broad range of legal issues. She is a frequent invited speaker in conferences and a member of study committees which recommend and draft policies and legislations.