Preface

Increasing every day in frequency and sophistication, planned cyber attacks are impacting systems, data and user access at virtually every business and government organization. Whether accidentally triggered by users opening their daily e-mail, or planned denial of services attack triggering a thousand zombie systems, IT management and corporate executives must be ready to respond, minimize and defeat threats to revenue generating and citizen facing operations. In many cases, the decision to protect information assets may materially impact agency or corporate budgets, previously planned investment and projected shareholder returns.

Edited by a senior IT executive with contributions from industry and government experts, this book is written for senior managers by senior managers. Avoiding technical jargon except when necessary, the book is organized into three primary sections of governance, architecture and technology. Each section provides extensive insights, including the legal, staffing, financial, communications, risk, management strategies and technical aspects of securing IT computing and communications systems. A decision framework is provided at the end of each chapter to assist in making the management trade-offs between investment, security, access and legal compliance. At the end of the book are reference lists of publicly available security related information sources.

Using the book's decision trade-off frameworks to make better decisions, executives and managers select which short-term and long-term investments and support activities are required to protect their computing infrastructures. Based on best practices from information assurance professionals and security consultants in government and industry, the unique decision trade-off frameworks describe processes, actions and budgets that effectively protect information and system access in a quickly changing and challenging world.

The **Executive Overview** discusses the *security as a process* concept that has gained recognition within the IT and security communities. Several topics reviewed include the new world of IT security, the continuously increasing value of information assets, and the security challenges and responsibilities facing executives and senior managers today.

Section I reviews the governance issues of IT security, including balancing employee privacy with information access, administrative security policies, legal exposures, risk management strategies and trusting trusted systems.

Section II introduces the architecture issues of IT security, starting with building a threat matrix. It then provides details on architecture alignment with service level agreements, constructing multilevel protection barriers, and revealing internal threats to IT security processes. The section also discusses disaster planning approaches.

Section III focuses on technology issues that intersect and support the issues of governance and architecture. Technology components comprise a large percentage of IT security investments, and executives need some understanding of how the technology is applied, how it functions and why it is so expensive to operate and maintain. This section reviews COTS software protections, data backup and restore, continuity planning, data obsolescence, biometrics, smartcards, and security penetration testing.

Reference Materials are provided as pointers to publicly available information security sources. As major legislative and technical standards

are expected in the coming years, checking these sources for updates on a quarterly basis is prudent and beneficial.