

Preface

Information technology (IT) infrastructure security is a complicated subject. Opportunistic attackers routinely exploit security vulnerabilities, which are easily identified and rarely fixed. Experienced security professionals usually address IT security. However, there are an increasing number of people that need to understand the fundamentals of security in a rapidly changing technology world. This book is written for governmental officials, management, IT management, and less experienced security administrators to help them understand and deal with existing security risks. The need for security planning is more evident today than ever before. Most experts believe that computer crime is increasing significantly. Exposure to computer crime is on the rise with the advent of elaborate communications networks, closely coupled computer systems, networks of all sizes, and users who are much more technically sophisticated than the users of previous years.

This book describes a methodology for security planning that focuses on risks, related threats, tools for addressing the threats, and the processes needed to build more secure systems and continuously monitor and improve security. The approach is based on a proven technique that results in documented security strategies and informed decisions. This book can be used as a guide for security “best practices” because it provides a wider perspective on security in general for better understanding how to reduce and manage security risk. Several forms, charts, and diagrams are included to facilitate performing the process in a logical and efficient manner.

We, the managing directors of LBL Technology Partners, appreciate the contribution of Stephanie W. Bollinger, who provided extraordinary effort in research, formatting, and organization.

Geoffrey H. Wold, CISA, CPA, CITP, CMA, CSP, CCP, CMC, CFSA, CIRM

Jeffrey S. Locketz, CISA, CISM, CPA, CITP, CBCP