Foreword

From a distance, the concept of e-commerce security seems simple. Just allow authorized people to transact business securely and efficiently through the Internet, and keep unauthorized people away from valuable information. But in today's impersonal and global economy, how can a business or organization really know who they are really allowing into their systems? And how can they be sure unauthorized people are always kept out?

In a highly interconnected and transaction-driven world, deciding who should be kept out or included is becoming more difficult every day. Due in part to interdependent global economic conditions, international terrorism concerns and human ingenuity involved with misusing technology for ill gotten gains, e-commerce security is neither simple nor static.

The managers and executives of companies and organizations that offer e-commerce access points must realize that security is no longer a part-time activity, performed when the IT staff has time each week to check a few system access logs and monitor unused network firewall ports. Around-the-clock monitoring using a combination of automated and human resources has become not only a good marketing story, but is now a business requirement to minimize financial losses and litigation. Inherently this means a dramatically different perspective from a few years ago about what the cost of, and mission focus should be, for the e-commerce security organization.

The definition of what "e-commerce" really means to the business or organization, its clients and its supplier/partners must also be reviewed for scope, clarity and security access. In the rush to be first-to-market a few years ago, important security features were often left out to make the schedule, and have not been addressed since. In other cases, the e-commerce front-end to back-office databases remain open to unauthorized access due to incomplete security architectures, dependence on computer operating system manufacturers, and/or perceived client "ease of use" features and functions.

Compounding the organization's e-commerce business processes and IT budgets is the dearth of industry security standards and plethora of often incompatible proprietary software and hardware products. Continually guessing at which technologies (and their developers) will survive the current market downturn has made selecting the best products suitable for their use very difficult. And last, while e-commerce security is required to protect business assets, as a general rule it is an overhead cost, not a revenue generator. As companies seek to reduce costs, security is often an area of downsizing due to a perceived risk of acceptable financial loss.

As mentioned earlier, e-commerce security is neither simple nor static. Elements of the complex answer are contained in the details of system management, business processes and security technology. Taking the unique approach of interviewing industry experts working on, and solving, complex e-commerce security problems and assignments, this book provides illuminating ideas and discussions about what management and industry practitioners can do to protect their companies and organizations based on best practices and what works. By applying these ideas to specific situations, management can greatly reduce the cost and time required to harden their systems to unapproved access and undesired financial risk.

The U.S. Government reports that several billions of dollars are lost every year to e-commerce and computer security crimes (2002 Computer

Crime and Security Survey Report)–an amount growing every day. Stopping that growth rate and driving it to zero will become a larger and larger management challenge and responsibility from the legal and financial perspectives.

Most books that have been written about e-commerce security lack a key ingredient–actual business examples from industry practitioners. This book seamlessly incorporates specific expert information throughout various chapters and sections, providing the reader with relevance and rare insights into current security threats and defenses faced by business leaders.

Compared to an industry research monologue, readers benefit from the experts' multi-decade experience dealing with e-commerce problems: security threat priorities, personal privacy laws, risk management and other at-risk tasks that impact revenue generation and collection. Usually obtainable only at extraordinary expense, readers can learn from and leverage industry best practices, thus saving significant time and expense, while reducing security risks for their organizations.

In the end, e-commerce security is not only about buying and installing technology and stopping unauthorized user access. It is about creating continuous business processes that wrap around and balance end-to-end system and user access, provide transaction security, and require proprietary and customer information to be considered valuable business assets.

Lawrence Oliva
Deputy Director
Infrastructure Engineering
CSC PRIME Alliance, USA