Preface

According to empirical studies by Williams (2004), the paradox in security expenditure between advanced and developing economies has resulted in a security gap. The irony is that while investments in security amongst IT companies in advanced economies are not that high in budget, the methods employed for assessing possible risks in the application of technologies are normally high in cost. This meant that investments in risk assessment were far higher than risk mitigation. On the contrary, investments in risk mitigation were higher than risk assessment amongst companies in developing economies.

The studies provided an insight into technologies that supported electronic transactions in international banking. Security bottlenecks experienced by end users were also assessed. Human ware was crucial to securing any system. It was found that authentication methods formed the nucleus of any security system. Authentication methods assured customers of key security goals such as confidentiality, integrity and availability. The studies showed that these security goals could be breached if authentication was compromised, unless identification and verification processes within authentication were improved and resolved with appropriate security measures and standards. In the financial sector, the absence of such measures makes information regarding a particular transaction available to attackers and intruders. This could result in a breach of confidentiality which is a key goal of security.

This book presents an overview and critique of online business security systems with emphasis on common electronic commerce activities and payment systems. It discusses legal, compliance and ethical issues that affect management and administration of online business systems. The book introduces the reader to concepts underlying online business systems, as well as technologies that drive online business processes. There is critical evaluation of infrastructure and technologies that support these systems. The role

of stakeholders and third parties such as banks, consumers, service providers, traders and regulatory bodies are discussed. Vulnerabilities associated with critical online business infrastructure are highlighted. There is a description of common attacks against online systems and a review of existing security and risk models for securing these systems. Finally this book presents a model and simulation of an integrated approach to security and risk management known as the (SSTM) Service Server Transmission Model for securing Online Business Systems.

http://www.springer.com/978-0-387-35771-3

Online Business Security Systems
Williams, G.B.
2007, XVIII, 220 p., Hardcover
ISBN: 978-0-387-35771-3