


xI	WELCOME
xII	HOW TO USE THIS BOOK


PERSPECTIVES

xv	
1	EXECUTIVE SUMMARY
7	RISK AND SHAREHOLDER VALUE
15	CREATING TRUST IN AN E-BUSINESS WORLD
35	INTERVIEW WITH FRANCIS GURRY
45	INTERVIEW WITH MARGARET JANE RADIN
53	INTERVIEW WITH ROBERT SIMONS
61	INTERVIEW WITH ROBERT VERRUE




CRITICAL ISSUES

71	
73	SECURING THE CONNECTED ENTERPRISE
91	DEPLOYING TRUST INFRASTRUCTURE
117	PRIVACY COMPLIANCE



ENABLING TECHNOLOGIES

147	
149	ENCRYPTION TECHNOLOGIES
185	BIOMETRICS AND TOKENS
217	SECURING IT PLATFORMS
253	SECURING REMOTE ACCESS



295	INDEX
------------	-------

LIST OF FIGURES

PERSPECTIVES	
9	Figure 1: Evolution of Risk Decision-Making
10	Figure 2: Benefits of Operational Risk Management
11	Figure 3: Business Attitudes Toward Risk
12	Figure 4: Phases in the Development of Operational Risk Management
14	Figure 5: Business Risk Continuum
17	Figure 6: Establishing a Trusting Relationship
25	Figure 7: The Three Elements of Risk
27	Figure 8: Factors Affecting Security Measures
28	Figure 9: Downtime Caused by Security Breaches or Espionage
30	Figure 10: Enterprise Security Priorities
41	Figure 11: Domain Name Dispute Case Filings: 2000
54	Figure 12: Risk Exposure Calculator
CRITICAL ISSUES	
74	Figure 13: ERP and B2B Development
77	Figure 14: The Integrated ERP System
80	Figure 15: Integrated Security Architecture
97	Figure 16: Third-Party Trust Through a Certificate Authority
98	Figure 17: Digital Signature Certification Process Flow
99	Figure 18: Certification Authority Hierarchy
102	Figure 19: Sample PKI Design
104	Figure 20: Validation Processing
112	Figure 21: CAGR for PKI Product and Services Market: 1999–2003
113	Figure 22: PKI Implementation Market Summary: 1999 and 2003 (millions of dollars)
114	Figure 23: PKI Vendor Positioning: 1999 and 2003
ENABLING TECHNOLOGIES	
150	Figure 24: A Cipher or Cryptosystem
152	Figure 25: The Caesar Cipher
153	Figure 26: The Spartan Cipher
159	Figure 27: A Symmetric Key Cryptosystem
161	Figure 28: A Transposition Cipher
161	Figure 29: Example of a Product Cipher
163	Figure 30: 3-DES
165	Figure 31: One-Time Pad Use
166	Figure 32: Public Key Encryption
172	Figure 33: A Digital Envelope
173	Figure 34: Man-in-the-Middle Attack
175	Figure 35: Digital Signature Plus Message Digest Scheme
178	Figure 36: A Certification Hierarchy
180	Figure 37: PGP's Web of Trust Model
187	Figure 38: Authentication Alternatives
189	Figure 39: A Smart Card Family Tree
190	Figure 40: A Smart Card and Its Interface Contacts
195	Figure 41: The CombiCard Contactless Integrated Circuit Architecture

205	Figure 42: TrueFace Screen
205	Figure 43: TrueFace ID Video
213	Figure 44: Worldwide Revenue by Type of Biometric Technology: 1999
214	Figure 45: The Effects of Combining Biometrics and Digital Certificates
229	Figure 46: CORBA Services
235	Figure 47: Kerberos Security
245	Figure 48: Enterprise Security Management Architecture
247	Figure 49: Security Software Market Leaders for New License Sales: 1999
249	Figure 50: Worldwide Object, Message, and TP Middleware Revenue: 1999–2004
255	Figure 51: Growth in the Number of Incidents Handled by the CERT/CC
255	Figure 52: Attack Sophistication vs. Intruder Technical Knowledge
257	Figure 53: Elements of Securing Remote Access
258	Figure 54: Remote Access Services
260	Figure 55: Sample VPN Packet
261	Figure 56: VPN Placement within the OSI 7-Layer Model
261	Figure 57: Providing VPN Remote Access
262	Figure 58: Providing VPN Branch Office Access
262	Figure 59: Providing VPN Business Partner/Supplier Access
267	Figure 60: Single-Homed Firewall
267	Figure 61: Multihomed Firewall
268	Figure 62: Packet Filter
268	Figure 63: Circuit-Level Gateway
269	Figure 64: Application-Level Gateway
270	Figure 65: Stateful Inspection Firewall
271	Figure 66: Firewall Security vs. Performance Tradeoff
274	Figure 67: IDS Characteristics
275	Figure 68: IDS Probability of Detection
281	Figure 69: VLANs Crossing Physical Boundaries
287	Figure 70: Secure WAP Session

LIST OF TABLES

PERSPECTIVES	26	Table 1: Risk Management Objective Matrix
	31	Table 2: Establishing the Foundation of a New Security Model
CRITICAL ISSUES	113	Table 3: PKI Product and Services Revenue: 1999–2003
	126	Table 4: Selected Privacy Lapses and Their Business Impact
	139	Table 5: Summary of Privacy Legislation in Europe
	143	Table 6: Comparison of U.S. Safe Harbor Principles and E.U. Data Protection Directive
ENABLING TECHNOLOGIES	162	Table 7: Product Cipher Characteristics
	170	Table 8: Size of an Encrypted 100-bit Message
	204	Table 9: Comparison of Biometric Technologies
	210	Table 10: Worldwide Shipments of Microprocessor and Memory Cards: 1998–1999
	211	Table 11: Worldwide Chip Card Production by Market Segment
	212	Table 12: Worldwide Network Security Smart Card Forecast: 1999–2004
	213	Table 13: Unit Sales and Average Prices of Biometric Devices in the U.S.: 1990–2000
	219	Table 14: Trend Toward Complexity in Source Code
	221	Table 15: Security Classifications
	246	Table 16: Security Market's New Software License Sales: 1998–2004
	248	Table 17: Worldwide Client Operating System Shipments: 1999
283	Table 18: Wireless Networks Coverage	
291	Table 19: Worldwide VA and IDS Software Revenue, Growth, and Share: 1999–2003	

PERSPECTIVES	50	Copyleft
	69	Export of Dual-Use Commodities
CRITICAL ISSUES	79	Models of Access Control
	93	PKIX
	94	Information Security Objectives of Cryptography
	120	International Privacy Initiatives
	121	Identity Theft
	124	Practical Implementation of Global Privacy Compliance
	132	Privacy and Surveillance
ENABLING TECHNOLOGIES	154	Bletchley Park, GCHQ, and Pre-PKI Government Research
	159	Randomness and Pseudo-Random Number Generators
	160	Modular Arithmetic
	163	XOR Logic Operation
	164	AES to Replace DES
	167	Classifying Hard Mathematical Problems
	169	Key Length
	170	Moore's Law
	171	Cracking DES
	191	Smart Card Standards
	223	TEMPEST Attacks
	232	What Really Happens with Passwords
	237	Denial-of-Service Attacks
	239	Content Security Monitoring
	244	Portal Security
	254	CERT/CC
	256	Security Management
259	Internet Building Blocks	
272	Incident Management	
276	Vulnerability Assessment and Intrusion Detection	