

Contents

Preface to the Third Edition	xiii
Preface to the Second Edition	xv
Acknowledgments	xvii

PART I THE THREAT TO COMPUTER SECURITY

Chapter 1	Essentials of Computer Security	3
	Unique EDP Security Problems	3
	EDP Security in a Nutshell	8
	Computers and Crime; Know Your Enemy!	13
	The Anatomy of Computer Crime	20
Chapter 2	Computer Crime and the Law	29
	United States	29
	Australia	32
	Canada	35
	United Kingdom	42
	New Zealand	44
	Continental Europe	44
	Conclusions	46
	Classic Case Histories	47
References for Part I		59

PART II SECURITY MANAGEMENT CONSIDERATIONS

Chapter 3	Organizing for EDP Security	65
	EDP Security in the Public Sector	65
	EDP Security in the Private Sector	66
	Corporate EDP Security	69
	Duties of the Security Coordinator	72
	Principles of Security Management	74
	New Challenges for IT Security Management	76

Chapter 4	Protection of Information	79
	Classification—The Government Model	79
	Classification—The Corporate Model	83
	Special Problems with EDP	85
	Marking Classified Matter	86
	Storing Classified Matter	88
	Destroying Classified Matter	89
	Residual Memory in Magnetic Media	90
	Procedural Safeguards for Classified Matter	92
	Conclusion	95
Chapter 5	Screening and Management of Personnel	99
	Management Responsibility	102
	Relations with Vendors	102
	Categories of Security Clearance	103
	Security Screening of Employees	104
	Personnel Security Policies	108
	Conclusion	111
PART III PHYSICAL SECURITY		
Chapter 6	Physical Access Control	115
	Basics of Access Control	115
	Automatic Access Control	116
	Key Access Control	120
	Concentric Controlled Perimeters	120
	Outer Perimeter Access	121
	Building Access Control	122
	Control of Access to Restricted Areas	123
	Material Control in Restricted Areas	126
	Computer Room Access Control	127
Chapter 7	Physical Security	131
	The Fortress Concept	131
	Outer Perimeter Defense	133
	Building Perimeters	134
	Guarded Areas	136
	Restricted Area Perimeter	139
	Computer Room Security	142
Chapter 8	Environmental Security	145
	Electrical Power	145
	Grounding	149
	Interference Suppression	150

	Dust Control	152
	Environmental Controls	153
Chapter 9	Disaster Control	157
	Locating the Computer Center	157
	Protecting the Computer Center	160
	Automatic Fire Detection	165
	General Fire-Safety Planning	167
	Disaster Recovery	169
 PART IV COMMUNICATIONS SECURITY		
Chapter 10	Line Security	177
	Communications Security Subfields	177
	Security of Communications Cables	178
	Interior Communications Lines	182
	Telephone Instrument Security	183
	Additional Line Security Considerations	188
	Local Area Networks	189
	Space Radio Interception	195
Chapter 11	Transmission Security	199
	General Considerations	199
	Operating Procedures	200
	Speech Privacy	206
	Error-Proof Codes	210
	Traffic Analysis	213
Chapter 12	Cryptographic Security	215
	Introduction to Cryptology	215
	Overview of Ciphers	216
	How Ciphers Work	219
	How DES Works	224
	Network Communications Security	235
	Weaknesses of DES	236
	Ways to Use DES	238
	Asymmetrical Ciphers	241
	El Gamel	243
	Crypto Procedures	244
	Cryptanalysis	246
	Summary	249
Chapter 13	Emanations Security	251
	Emission Problems	251
	Probability of Interception	253
	Defense Mechanisms	254

	Measuring Electromagnetic Emanation Levels	256
	Additional Defenses	260
	Defense Against Acoustical Emanations	265
Chapter 14	Technical Security	267
	Victimization of EDP Centers	267
	Categories of Technical Surveillance	268
	Defenses Against Technical Surveillance	269
	Types of Intrusion Devices	273
PART V SYSTEMS SECURITY		
Chapter 15	Systems Identification	281
	Introduction to Systems Security	281
	Guidelines for a Trusted Computing Base	286
	Personal Identification	291
	Other User Identification Systems	298
	Identifying Specified Assets	298
	System Relationships	302
	Privacy Considerations	302
	Freedom of Information	304
Chapter 16	Isolation in Computer Systems	307
	Defense Strategies	307
	Processing Modes	308
	Temporal Isolation	310
	Spatial Isolation	312
	System Architecture	312
	Cryptographic Isolation	325
	Restriction of Privilege	326
	Virtual Machine Isolation	327
	Trends in User Isolation	327
Chapter 17	Systems Access Control	329
	Basic Principles of Access	329
	Authentication	332
	Systems Access	336
	Internal Access	337
	Access Privileges	340
	Keeping Hackers Out	344
	System Security Add-on Packages	349
Chapter 18	Detection and Surveillance	353
	Threat Monitoring	353
	Trend Analysis	355

	Investigation	361
	Auditing	363
	Compensatory Action	365
	The Human Factor in Computer Crime	367
Chapter 19	Systems Integrity	369
	Program Security	369
	Error Control	372
	Privacy in Statistical Data Bases	375
	Protection of Security Functions	379
	Commercial Security Model	381
	Object-Oriented Model	383
	Conclusion	386
	Bibliography	387
Chapter 20	Systems Reliability and Security	389
	Hardware	389
	Software	391
	Changes	392
	System Backup	392
	Record-Keeping and Security	395
	Logs	395
	Backup Files	397
	Restart and Recovery	398
	Record Retention	399
	Inventories and Lists	400
Chapter 21	Security and Personal Computers	403
	Introduction	403
	Physical Security	405
	Environmental Protection	407
	Protection of Removable Media	409
	Electromagnetic Emanations	412
	Security Attributes of Microprocessors	412
	PC Operating Systems	417
	Local-Area-Network (LAN) Security	428
	Security in Remote Support Programs	431
	Database Security	434
	Security in Application Programs	438
	Backup	439
	Anti-Virus Defenses	443
	Security Add-ons for PC Operating Systems—Trusted Computer Systems	
	Evaluation	447
	New Thinking in PC Security	453

Conclusion	456
Bibliography	456

PART VI INFORMATION SECURITY RISK ANALYSIS

Chapter 22	Systems Approach to Risk Management	459
	Introduction	459
	Applications of Risk Analysis	459
	IT Security Management	460
	Information and Risk Analysis	462
	Information Security by Consensus	462
	State of Infosec Risk Analysis	464
	General Systems Approach	464
	Cybernetic Control Cycle	466
	Problems in Risk Analysis	466
	Cybernetic Model of Activity	467
	Representative Risk-Analysis Packages	471
	Specific Recommendations	473
Chapter 23	Threat Assessment	477
	Introduction	477
	Properties of Threats	479
	Estimating Likelihood	482
	Trend Analysis	487
Chapter 24	Assets and Safeguards	491
	Assets	491
	Vulnerabilities	492
	Assets and Impacts	493
	Risk-Analysis Modeling	493
	Cost-of-Loss Model	497
	Safeguards	500
	Constraints	502
Chapter 25	Keeping Secrets in Computers	505
	Threats and Legal Remedies	506
	Self-Help Measures	509
	National Security Models	511
	Threat Risk Assessment	539
Chapter 26	Modes of Risk Analysis	547
	Compliance Auditing	547
	Requirements Analysis	548
	Security Inspection and Evaluation	551
	Cost-Benefit Analysis	553
	Life-Cycle Software Development	556

Development of Security Software	557
The Workshop Model	558
Transaction Model	562
References for Part VI	569
Appendix: Sample Log Forms	575
Glossary	579
Selected Bibliography	629
Index	635