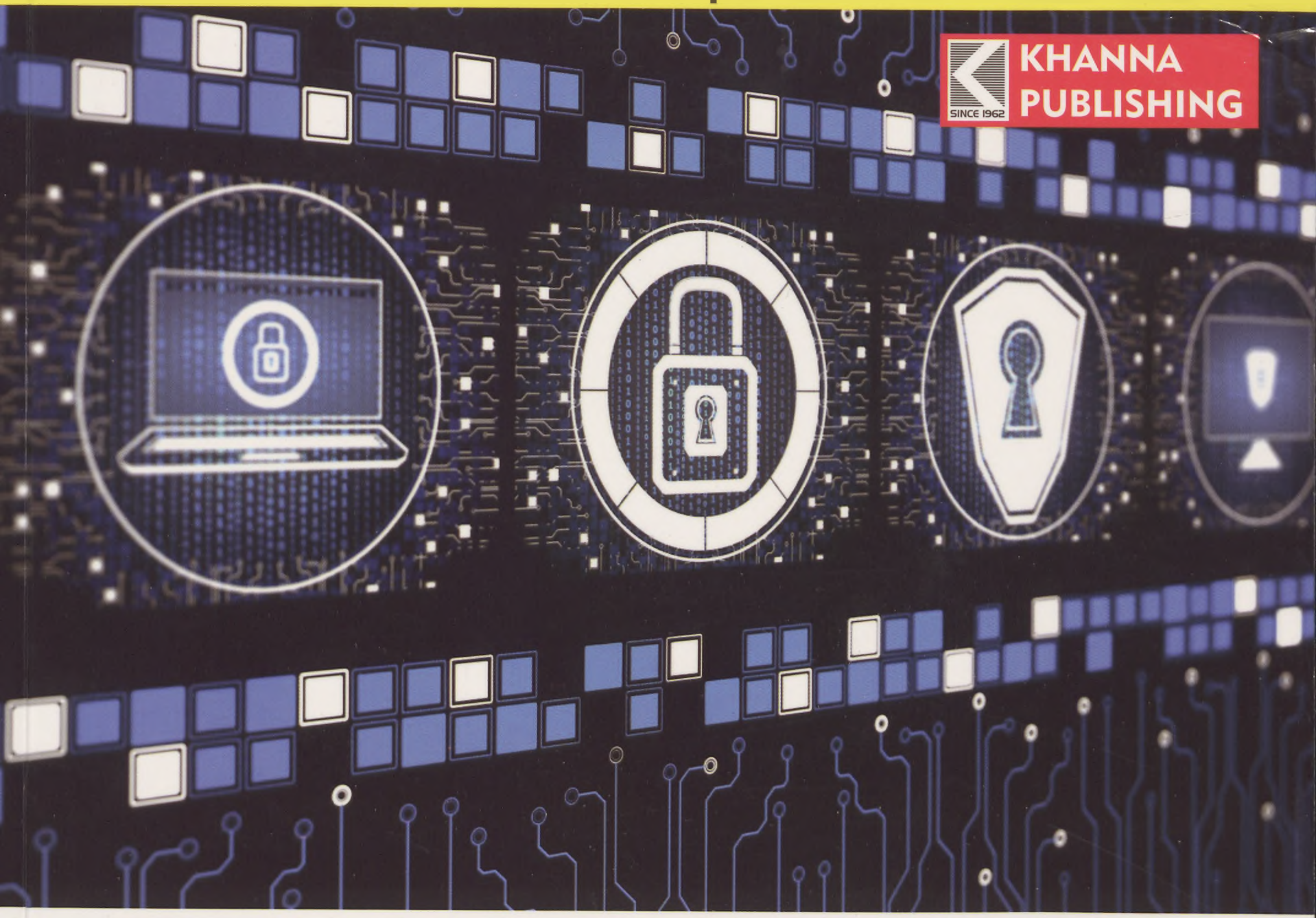
AICTE Recommended Textbook as per Model Curriculum -2018

KHANNA
PUBLISHING
SINCE 1962



INFORMATION SECURITY *and* CYBER LAWS

SARIKA GUPTA ▪ GAURAV GUPTA

INFORMATION SECURITY *and* CYBER LAWS

INFORMATION SECURITY *and* CYBER LAWS

BIBLIOTEKA
Nr ewid. ....
Akademii Sztuki Wojennej

SARIKA GUPTA
Asstt. Prof.
MCA. M.Tech, MBA, Ph.D(CSE)
CSE/IT Deptt. Dronacharya College of Engineering
Greater Noida, Uttar Pradesh (INDIA)

ER. GAURAV GUPTA
Manager Client Services
Rightwave Info. Solution Pvt. Ltd.
NOIDA

KHANNA BOOK PUBLISHING CO. (P) LTD.
Publisher of Engineering and Computer Books
4C/4344, Ansari Road, Darya Ganj, New Delhi-110002
Phone : 011-23244447-48 **Mobile:** +91-9910909320
E-mail : contact@khannabooks.com
Website : www.khannabooks.com

Price: ₹ 335.00

INFORMATION SECURITY *and* CYBER LAWS

Sarika Gupta, Gaurav Gupta

Copyright © Khanna Book Publishing Co. (P) Ltd.

This book is sold subject to the condition that it shall not, by way of trade or otherwise, be lent, resold, hired out, or otherwise circulated without the publisher's prior consent in any form of binding or cover other than that in which it is published and without a similar condition including this condition being imposed on the subsequent purchaser and without limiting the rights under copyright reserved above, no part of this publication may be reproduced, stored in or introduced into retrieval system, or transmitted any form or by any means (electronic, mechanical, photocopying, recording or otherwise), without the prior written permission of both the copyright owner and the above mentioned publisher of this book.

ISBN: 978-93-81068-24-3

First Edition: 2013
Reprint: 2019

Published by:

Khanna Book Publishing Co. (P) Ltd.
4C/4344, Ansari Road, Darya Ganj, New Delhi-110 002
Phone: 011-23244447-48 **Mobile:** +91-9910909320
E-mail: contact@khannabooks.com

Printed in India by:
S.P.S. Printers & Binders, Delhi

This book is dedicated to-

OUR FAMILY

Preface

It gives us great pleasure in presenting the first edition of this book to our esteemed readers. "**Information Security and Cyber Law**" is written with several goal in mind. It is designed to provide all essential information you'll need to learn **ISCL**. It can be used as a test-cum-reference book by students of B.Tech (CS/IT) / MCA and M.Tech.

I am sure that the text's user friendly approach will encourage the students to read the book and will make them understand the concept in easy way.

We always welcome emails with comments and suggestions from researchers, academicians, students and other to improve the quality of this book.

Sarika Gupta
Gaurav Gupta
togupta.gupta@yahoo.co.in

Contents

UNIT-1

1. What is Information **3–65**

1.1 What is a System 3

1.1.1 Definition of System 3

1.2 Classification of System 4

1.2.1 Physical or Abstract System 4

1.2.2 Open Closed System 4

1.2.3 Man made Information System 4

1.3 Analytical Representation of a System 5

1.4 System Components and Characteristics 6

1.4.1 Resources 6

1.4.2 Procedures 6

1.4.3 Data/Information 6

1.4.4 Intermediate Data 7

1.4.5 Processes 7

1.5 What is an Information system 8

1.6 Differences between System and Information System 9

1.7 Types of Information Systems 10

1.7.1 Transaction Processing Systems 10

1.7.2 Management Information Systems 10

1.7.3 Decision Support Systems 10

1.8 History of Information System 12

1.9 Summary of Information Systems 12

1.10 Global Information Systems 12
1.11 Components of Information Systems 14
1.11.1 Computer Hardware 14
1.11.2 Computer Software 15
1.11.3 Databases 15
1.11.4 Telecommunications 15
1.11.5 Human Resources and Procedures 15
1.12 Categories of IS 16
1.12.1 Operational Support 16
1.12.2 Support of Knowledge Work 16
1.13 Acquiring information systems 18
1.13.1 Acquisition from External Sources 18
1.13.2 In-house Development 18
1.14 Managing Information Systems 18
1.14.1 Information System Infrastructure and Architecture 18
1.14.2 Organization of Information Services 19
1.15 The Importance of Information Systems 19
1.15.1 Information is an Asset for Organizations 20
1.16 Benefits of an Information System 23
1.16.1 Where Information Systems Used 23
1.16.2 Introduction to Information Systems - Technology 23
1.16.3 Introduction to Information Systems - Networks 24
1.16.4 Introduction to Information Systems - Applications 24
1.16.5 Introduction to Information Systems - Development 25
1.17 Differentiating IS from Related Disciplines 25
1.18 Levels of information system 26
1.19 Purpose of information system 26
1.20 Basics of IS 27
1.20.1 Hardware 27
1.20.2 Software 27
1.20.3 Data 28
1.20.4 Methods of Data Access 29
1.20.5 Maintaining Data of an Organization 30
1.20.6 Using a Database System 30

1.20.7 People 30

1.20.8 Providers of Information Services 30

1.20.9 Users of Information 30

1.20.10 Abuse of Information Systems 31

1.20.11 Reason Why do Organizations Need Information Systems 31

1.21 Changing Nature of Information System 32

1.22 Function of IS 32

1.22.1 Information Processing and Usability Function 33

1.22.2 Educating and Learning Function 33

1.22.3 Information Systems Development Function (Methodologies) 34

1.22.4 Management and Control Function 34

1.22.5 Strategy & Planning Function 35

1.23 Examples of Information Systems, Inputs, Outputs, and Processing 37

1.24 Role of Information system 38

1.24.1 Information Flow in an Organization 38

1.25 Pattern of Processing 39

1.26 Where Information System is Used 39

1.27 Some of the advantages of information System 39

1.28 Some Disadvantages of Information System 40

1.29 Reason to Use Information System in Business Today 41

1.30 Information Systems Foundation for Conducting Business 42

1.30.1 Process Improvement 42

1.30.2 Cost Reduction 43

1.30.3 Quality Assurance 43

1.30.4 Communications 43

1.30.5 Competitive Intelligence 43

1.31 Business Environment in IS 43

1.32 Distributed Information System 44

1.33 Need of Distributed Information System 44

1.34 Advantages of Distributed Systems over Centralized Ones 48

1.35 Disadvantages of Distributed Systems over Centralized Ones 49

1.36 Role of Internet and Web Services 49

1.36.1 What is Web 49

1.36.2 Web Services 49

1.36.3 Reason to Use Web Services 50
1.36.4 Convincing the Boss 50
1.36.5 Role of Internet 51
1.37 Information System Threats and Attacks Defined 51
1.37.1 Threats 51
1.37.2 Accidental Threats 53
1.37.3 Type of Attacks 53
1.37.4 Passive Attacks 53
1.37.5 Active Attack 54
1.37.6 Covert Channels 54
1.37.7 Dealing with Attacks 55
1.37.8 Physical Access Security 56
1.37.9 Login / Password Security 56
1.37.10 Anti-Virus Software 56
1.37.11 Remote Access Security 57
1.38 Information System Security 57
1.39 Classification of security threats and Accessing Damages 58
1.39.1 Physical Threat 58
1.39.2 Accidental Error 58
1.39.3 Unauthorized Access 59
1.39.4 Malicious Misuse 59
1.40 Accessing Damages 59
1.41 Brief review of Internet Protocols-TCP/IP, IPV4, IPV6 61
1.42 Functions of Various Networking Components-routers, Bridges, Switches, Hub, Gateway And Modulation Technique 62
Summary 64
Exercises 65
2. What is Security 66–94
2.1 Introduction 66
2.1.1 Security Architecture 66
2.2 Wireless Security 67
2.3 Security Goals Technically Defined 68
2.4 Security Services – Overview 69
2.4.1 Authentication 69

2.4.2 Integrity 69

2.4.3 Confidentiality 69

2.4.4 Access Control 69

2.4.5 Non Repudiation 69

2.4.6 Wireless communication 69

2.5 Information Security Risks 70

2.6 Security in Mobile and Wireless Computing 71

2.7 Security Aspects of Mobile Communication 72

2.8 Securing Challenges in Mobile Devices 73

2.8.1 Mobile Devices 73

2.9 Characteristics of Mobile Devices 75

2.9.1 Portability 75

2.9.2 Small Size 76

2.9.3 Wireless Communication 76

2.9.4 Mobile Device Vulnerabilities 76

2.10 Mobile Application 77

2.10.1 RFID 79

2.11 Information Systems Security and Control 81

2.11.1 Information Systems Security 81

2.11.2 Computer Crime and Abuse 81

2.11.3 Securing Information 82

2.11.4 Organizational Impacts of Information Systems 82

2.12 Authentication Service Security 82

2.13 Security Levels of Mobile Communications 83

2.14 Implementing Secure Mobile Communications 85

2.15 Technical and other Challenges and Limitations of Mobile Computing 87

2.15.1 Insufficient Bandwidth 87

2.15.2 Security Standards 88

2.15.3 Power Consumption 88

2.15.4 Transmission Interferences 88

2.15.5 Potential Health Hazards 88

2.15.6 Human Interface with Device 88

2.16 Security Implication for Organization 88

2.17 Laptops Security and Basic Principles of Information Security 90

2.17.1 Confidentiality 90

2.17.2 Integrity 90

2.17.3 Availability 91

2.17.4 Authenticity 91

2.17.5 Non-repudiation 91

2.18 Information Classification and their Roles 91

2.18.1 Security Classification for Information 91

2.19 Security Challenges in the Future Mobile Internet 92

Summary 93

Exercises 94

UNIT-2

3. What is E-commerce 97–158

3.1 Introduction 97

3.1.1 Type of E-commerce 98

3.1.2 How E-commerce Works 99

3.2 E-commerce Technology 100

3.2.1 The Benefits of E-commerce 100

3.2.2 Ecommerce Security Issues 101

3.2.3 Digital Signatures and Certificates 102

3.2.4 Secure Socket Layers 102

3.2.5 PCI, SET, Firewalls and Kerberos 102

3.2.6 Transactions 103

3.2.7 Practical Consequences 103

3.3 Security Issues in Electronic Commerce on Web 104

3.3.1 Security Risks in eBusiness 104

3.3.2 Criminal vs. Civil Laws 105

3.3.3 Privacy and Security Issues in E-Commerce 105

3.3.4 Security Vulnerabilities in Electronic Commerce 105

3.4 Security technologies 106

3.4.1 Economic Issues 107

3.4.2 e-Commerce Security: Attacks and Preventive Strategies 107

3.5 Security Threats to Electronic Commerce 107

3.5.1 Identifying e-commerce Threats and Vulnerabilities 108
3.5.2 What are the Threats 108
3.5.3 E-commerce Systems Risk Assessment 109
3.6 E-commerce Security Issues 109
3.6.1 Threats from Hackers and the Risks to Business 109
3.6.2 Impact of a Security Incident on the Business 110
3.7 Security Overview 110
3.7.1 The Players 111
3.7.2 Security Audits 111
3.8 Security Features 113
3.8.1 The Criminal Incentive 114
3.8.2 Points the Attacker Can Target 115
3.9 Attacks 115
3.9.1 Tricking the Shopper 115
3.9.2 Snooping the Shopper's Computer 116
3.9.3 Sniffing the Network 116
3.9.4 Guessing Passwords 117
3.9.5 Using Denial of Service Attacks 117
3.9.6 Using known Server Bugs 118
3.9.7 Using Server Root Exploits 118
3.9.8 Defenses 118
3.9.9 Education 119
3.9.10 Personal Firewalls 119
3.9.11 Secure Socket Layer (SSL) 120
3.9.12 Server Firewalls 121
3.9.13 Password Policies 121
3.9.14 Intrusion Detection and Audits of Security Logs 122
3.10 Security Policies and Standards 123
3.10.1 Using Cookies 123
3.10.2 Using Threat Models to Prevent Exploits 124
3.10.3 Responding to Security Issues 125
3.10.4 Using an Online Security Checklist 125
3.11 Web Services Introduction 128
3.11.1 Why Web Services 128

3.12 Top Five Security Issues (Expected) 128

3.12.1 Business Challenges 129

3.12.2 Security Issues 129

3.13 Features of security in Terms of Information System 130

3.13.1 What is the Security Perimeter 130

3.14 Virtual Ogranizations 131

3.14.1 Reasons Behind a VO 131

3.14.2 What Does "virtuality" Imply 131

3.14.3 Characteristics of a VO 132

3.14.4 VO Lifecycle 132

3.14.5 Benefits and Challenges of VOs 133

3.15 Business Transaction on Web 135

3.15.1 Examples of Business Transactions 135

3.15.2 General Requirements 136

3.16 E Governance and EDI 138

3.16.1 What is E-Governance 138

3.16.2 Why introduced EGovernances 139

3.17 Electronic Data Interchange (EDI) 139

3.17.1 Benefits of EDI 143

3.17.2 How does the EDI Process Work in the Retail Environment? 143

3.18 Electronic Payment 144

3.18.1 Concept and Size of Electronic Payment 145

3.18.2 Size of Electronic Payments 145

3.18.3 Conventional vs. Electronic Payment System 146

3.18.4 Process of Electronic Payment System 147

3.18.5 Payment Instructions 148

3.19 Types of Electronic Payment Systems 149

3.20 Online Credit Card Payment System 149

3.21 Electronic Cheque Payment System 150

3.22 Electronic Cash Payment System 152

3.23 Smart Cards based Electronic Payment System 152

3.24 Magnetic Strip and Digital Token 153

3.25 Success Factors of E-commerce Payment System 154

3.26 Comparison of Electronic Payment Systems 154

Summary 157

Exercises 158

4. Physical Security **159–196**

4.1 Introduction 159

4.2 Physical Security Plan Components 160

4.3 Disaster and Control 160

4.3.1 Natural Disaster 160

4.3.2 Earthquakes 161

4.3.3 Lahars 161

4.3.4 Hurricanes 161

4.3.5 Tsunami 161

4.3.6 Tornadoes 162

4.3.7 Volcano 162

4.3.8 Drought 162

4.4 Basic Tenets of Physical Security 164

4.4.1 Seven Elements of Highly Effective Security Policies 165

4.5 Physical Entry Control 166

4.6 Access Control Overview 167

4.6.1 Certificates Overview 167

4.6.2 Server Certificates 167

4.6.3 Client Certificates 167

4.6.4 Encryption Overview 168

4.7 Access Control 168

4.7.1 What are Biometrics 168

4.7.2 How Biometrics Works 171

4.7.3 What are Biometric Systems Used For? 172

4.7.4 Principles of Fingerprint Biometrics 173

4.7.5 How does Fingerprint Biometrics Work 173

4.7.6 Iris 173

4.7.7 Retina 174

4.7.8 Hand 174

4.7.9 Palm vein 175

4.7.10 Face 175

4.8 Criteria for Selection of Biometrics 176

4.9 Design Issues in Biometric Systems 176

4.10 Problems of Interoperability 177

4.10.1 The Cost of ID Cards 178

4.10.2 Legal Problems with ID Database 178

4.11 Economic and Social Aspect of Biometrics 178

4.12 Biometric Systems Offer Many Important Benefits 179

4.12.1 Why are Biometrics Secure 179

4.12.2 What are the Advantages and Disadvantages of Biometric 179

4.13 Factors in Biometrics 181

4.14 Critical Factors in the Assessment of Biometric Products 182

4.14.1 Matching Accuracy 182

4.14.2 Failure-to-Acquire ("FTA") Rate 182

4.14.3 System Throughput 183

4.14.4 Ease-of-Use 183

4.14.5 Appropriate Concept of Operations 184

4.15 Biometric Authentication 184

4.16 The Problem with Biometric Systems 185

4.16.1 Recognition Errors 185

4.16.2 Compromised Biometric Data 185

4.17 Biometrics Issues 186

4.17.1 Security 186

4.17.2 Privacy 187

4.17.3 Interoperability 187

4.17.4 Costs 187

4.18 Social Aspects 188

4.18.1 Clarity of Purpose in Relation to Biometric Applications 188

4.18.2 Interoperability and Equivalence of Performance and Process 188

4.18.3 Human Factors, Usability and Social Exclusion 188

4.18.4 Impact upon the Trust Model Between Citizen and State 188

4.19 Economic Aspects 188

4.19.1 The Concept of Optimal Identity 189

4.19.2 Negative Implications of Stronger Identification 189

4.19.3 Interoperability is Vital for Market Operation 189

4.19.4 Biometrics-related IPRs Threaten Open Competition 189

4.19.5 Public Sector uptake will Shape the Market 189
4.20 Legal Aspects and Challenges 189
4.20.1 Enabling Legal Environment 190
4.20.2 Opacity/Transparency Rules Required 190
4.20.3 Wider Implementation Raises Fundamental Concerns 190
4.20.4 Use of Biometrics in Law Enforcement 190
4.20.5 Technological Aspects 190
4.20.6 Performance/Accuracy 190
4.20.7 Biometric Privacy 191
4.20.8 Interoperability 191
4.20.9 Multimodality 191
4.20.10 Medical Aspects 191
4.20.11 Direct Medical Implications 191
4.20.12 Indirect Medical Implications 192
4.21 Features of Biometric Identification 192
4.21.1 The Seven Pillars 193
4.21.2 Biometric Application Types 193
4.21.3 Verification (1-to-1 matching) 193
4.21.4 Verification with Centralised Storage 194
4.21.5 Verification with Distributed Storage 194
4.21.6 Identification (1-to-many Matching) 194
4.22 Legal Challenges 194
Summary 195
Exercises 196

UNIT-3

5. Cryptography 199–248
5.1 Introduction 199
5.1.1 Important Terms in Cryptography 199
5.1.2 Types of Cryptography 199
5.1.3 The Goal of Cryptography 200
5.2 What is Encryption 202
5.3 Encryption Techniques 202

6.2.1 Network Security Model (NSM) 250
6.2.2 Why do We Need a Network Security Model 250
6.2.3 What is the Physical Layer 251
6.2.4 Elements of the Physical Layer 251
6.2.5 What is the VLAN Layer 252
6.2.6 What is the ACL Layer 252
6.2.7 What is the Software Layer 252
6.2.8 What is the User Layer 252
6.2.9 What is the Administrative Layer 253
6.2.10 What is the IT Department Layer 253
6.3 Perimeter Protection 253
6.4 Network Security Dimension 255
6.4.1 Security Management 255
6.4.2 Small Homes 255
6.4.3 Medium Businesses 256
6.4.4 Large Businesses 256
6.4.5 School 256
6.4.6 Large Government 256
6.5 Network Security Architecture 257
6.5.1 Phase One: Basic secure network 258
6.5.2 Phase Two: Autonomic Network 259
6.5.3 Phase Three: Authenticated network 260
6.6 Intrusion Detection 261
6.6.1 The Need for Intrusion Detection 263
6.7 Need for Network Monitoring for Intrusion Detection 263
6.7.1 Network Monitoring 264
6.7.2 Traffic Analysis 265
6.7.3 Two Primary Types of HIDS can be Distinguished 268
6.7.4 Audit Trail Processing vs. On-the-fly Processing 269
6.7.5 Audit Trail Processing 269
6.7.6 On-the Fly Processing 271
6.7.7 Anomaly vs. Signature Detection 272
6.7.8 Normal Behavior Patterns Anomaly Detection 272
6.7.9 Misbehavior Signatures - Signature Detection 273

6.8 Understanding Network Attacks 277

6.8.1 What is Hacking 280

6.8.2 What are Hackers or Network Attackers 282

6.8.3 The Common Types of Network Attacks 283

6.8.5 What are Viruses 288

6.8.6 What are Worms 289

6.8.7 What are Trojan Horses 290

6.8.8 Predicting Network Threats 290

6.8.9 Identifying Threats to DHCP Implementations 291

6.8.10 Identifying Threats to DNS Implementations 292

6.8.11 Identifying Threats to Internet Information Server (IIS) Servers 292

6.8.12 Identifying Threats to Wireless Networks 294

6.8.13 Determining Security Requirements for Different Data Types 295

6.8.14 Creating an Incidence Response Plan 295

6.9 Virtual Private Network 296

6.9.1 Common Uses of VPNs 298

6.9.2 Basic VPN Requirements 300

6.9.3 What Types of VPNs Are There 300

6.10 Need of VPN 302

6.10.1 How does VPN work 303

6.11 Use of Tunneling with VPN 304

6.11.1 Virtual Network Types 306

6.11.2 Internet-based VPNs 306

6.11.3 Intranet-based VPNs 308

6.12 Authentication-mechanism (VPN) 310

6.12.1 VPN Authentication - Secure Remote Access with eToken 310

6.12.2 eToken Provides the Best Secure Access to Your VPN 311

6.13 The Four Types of VPN Secure Dialog 311

6.13.1 Authentication (Access Control) 311

6.13.2 Presentation (Privacy /Encryption) 311

6.13.3 Transportation (Data Integrity) 311

6.13.4 Non repudiation (Correct Message Reception) 311

6.14 Security Concern in VPN 313

6.15 Need of Intrusion Monitoring and Detection 315

6.15.1 NIDS 315
6.15.2 HIDS 315
6.15.3 Signature Based 315
6.15.4 Anomaly Based 316
Summary 316
Exercises 317

UNIT-4

7. Security Metrics 321–356
7.1 What is Security Metrics 321
7.1.1 Information Security Metrics Concept 322
7.2 Security Metrics Classifications 322
7.2.1 Methods of Measurement Include 323
7.2.2 Technical Information Security Metrics 325
7.2.3 Organizational Information Security Metrics 325
7.2.4 Operational Information Security Metrics 326
7.2.5 Problems in Application of Metrics in Information Security 327
7.2.6 Nature of Information Security Issues 327
7.2.7 Security Objectives 328
7.2.8 Security Requirements 328
7.2.9 Building a Security Metrics Program 330
7.2.10 What Kind of Security Objectives Cause the Need for IS Metrics 331
7.2.11 Metrics Implementation 332
7.2.12 Need for IS metrics 334
7.3 The Benefits of Security Metrics 337
7.3.1 Why Metrics Generation Is Difficult 338
7.4 Building a Security Metrics Program with its Classification 339
7.4.1 Conclusion 342
7.5 Information Security and Law 343
7.5.1 Information Security 343
7.5.2 Part One: Protecting Private Sector Systems; Information Security Professionals and Trade Secrets 344
7.5.3 Computer Fraud and Abuse Act (CFAA) 344

7.5.3 DMCA - The Digital Millennium Copyright Act 345
7.5.4 State Laws - Filling the Gaps Left by CFAA and DMCA 346
7.5.5 Proprietary Information - Information Security Professionals and Trade Secrets 346
7.5.6 Security Principles 347
7.5.7 Trust 347
7.5.8 Authentication 348
7.5.9 Chain of Authority 348
7.5.10 Accountability 349
7.6 Intellectual Property Rights (IPR) Law in India 349
7.7 Patent Law 352
7.8 Copyright Law 352
7.9 Legal Issue in Data Mining 354
7.10 Plagiarism 354
Summary 356
Exercise 356

8. Ethical Issues 357–378

8.1 Ethics 357
8.2 Issue 358
8.3 Ethical Issues 358
8.3.1 Ethics and Responsible Decision-Making 358
8.3.2 Confidentiality and Privacy 358
8.3.3 Piracy 359
8.3.4 Fraud and Misuse 359
8.3.5 Liability 359
8.3.6 Patent and Copyright Law 360
8.3.7 Trade Secrets 360
8.3.8 Sabotage 361
8.4 Issues in Data and Software Privacy 361
8.4.1 Does India have Sufficient Laws 361
8.5 What is Cyber crime 362
8.5.1 Distinction Between Conventional and Cyber Crime 363
8.5.2 Mode and Manner of Commiting Cyber Crime 364
8.5.3 Classification of Cybercrime 366

8.5.4 Types of Cyber Crime 367
8.5.5 Prevention Methods 368
8.5.6 Information Security and Cyber Law 369
8.5.7 Cyber Law Issues in E-Business Management 370
8.5.8 Overview of Indian IT Act 371
8.5.9 Data Pprivacy and Protection 372
8.5.10 Domain Name 375
8.5.11 Issues in Ethical Hacking 376
Summary 377
Exercise 378
Question Bank **379–384**
Model Papers **385–387**
Question Papers **388–391**
Index **393–396**

PRINTED ON RECYCLED PAPER • PRINTED ON RECYCLED PAPER

Biblioteka Główna
Akademii Sztuki Wojennej
26654/III (CB)
03-026654-000-0

INFORMATION SECURITY *and* CYBER LAWS

Introduction of **Information Security and Security and Cyber Law** covers the Fundamentals Aspect of System, Information System, Distributed Information System, Cryptography, Network Security etc. It is Incredibly robust, portable & adaptable. This book coverage of Model Paper, Question Bank and Examination Question Paper etc.

CHAPTERS COVERED

- What is Information
- What is Security
- What is E-commerce
- Physical Security
- Cryptography
- Network Security
- Security Metrics
- Ethical Issues

KHANNA BOOK PUBLISHING CO. (P) LTD.
Publisher of Science, Technology and Engineering Books
4C/4344, Ansari Road, Darya Ganj, New Delhi - 110002
Phone: 011-23244447-48, **Mobile:** +91-99109 09320
E-mail: contact@khannabooks.com
Website: www.khannabooks.com

ISBN 10: 93-81068-24-0
ISBN 13: 978-93-81068-24-3
9 789381 068243