

Contents

Preface v

Acknowledgement vi

Syllabi–Book Mapping vii

1. Introduction to Information Security	1–20
Learning Objectives	1
Introduction	1
Information Security	3
The History of Information Security	3
The 1960s	4
The 1970s and 80s	4
Need for Information System	5
Role of Internet and Web Services	6
Mobile Devices and Wireless Communication	7
GSM Security	9
SIM Card	14
Threats—Classification and Assessment	14
Classification of Threats and Assessing Damages	16
Additional Related Concepts	17
Need of Distributed Information Systems	18
Summary	18
Questions and Answers	18
Exercise	20
 2. Organizational Security	 43–69
Learning Objectives	21
Introduction	21
Need for Physical Security	22
The Basic Tenets/Principles of Physical Security	23
Physical Security Mechanisms	23
Electronic Information	24
Confidentiality of Files	26
Identification and Authentication	26
Areas Where Physical Security Measures are Essential	27
Physical Reconnaissance	28
Physical Attack Methods	29
Loss of Access to Physical Systems	29
Laptop Security	29

Biometrics	30
Factors that Affect Biometric systems	32
Physiological Characteristics	33
Behavioral Characteristics	33
Access Control	34
Design Issues in Biometric Systems	35
Interoperability Issues	36
Social and Legal Issues in the Use of Biometrics	36
Security Threats	37
Natural Disasters	37
Environmental Threats	38
Technical Threats	40
Human-caused Physical Threats	40
Summary	41
Questions and Answers	41
Exercise	42
3. eCommerce	43–69
Learning Objectives	43
Introduction	43
The Goals of Security in eCommerce	44
Virtual Organization	45
Business Transactions on Web	45
Planning	46
XML-based Concepts	46
Concept of eCash	47
Perception of security	47
Security as a Restriction	47
Security as an Enabler	48
eCommerce Site Component	48
Business Transactions	50
User Anonymity and Location Untraceability	50
Payment Transaction Untraceability	52
Secure Transactions	55
Credit, Charge or Debit Cards	55
Approaches to Payments via the Internet	59
Commercial Payment Solutions Options	60
Secure Payment Processing Environments	60
Web Server Security	61
Common Gateway Interface (CGI)	62
Servlets	62
Database Security	63
Copyright Protection	64
Electronic Data Interchange and eGovernance	65
Summary	66
Questions and Answers	67
Exercise	69

4. Cryptography	70–105
Learning Objectives	70
Introduction	70
Definition and Meaning	71
How Cryptography is Done	71
Cryptanalysis is the Converse Process of Cryptography	71
Methods of Encrypting	71
Substitution Method	72
Transposition Method	72
Famous Cryptographic Devices	72
Enigma	73
Attacks against Encryption	73
Ciphers	74
Block Ciphers	77
Private Key Encryption	79
What is Private Key Encryption?	79
Public Key Encryption	84
What is Public Key Encryption	84
Diffie-Hellman	85
RSA algorithm	86
Generating RSA Keys	86
Worked RSA Example	86
RSA Today	87
Other Public Key Algorithms	87
The XOR Cipher and Logical Operands	90
Digital Signatures	91
What is a Digital Signature?	92
Need for Digital Signature System	93
Key Management	93
Key Creation	94
Key Distribution	94
Key Certification	95
Key Protection	96
Key Revocation	96
Trust	96
Hierarchy	97
Revocation of Certificates	98
Web	98
Traffic Padding Mechanisms	99
Message Freshness	100
Random Numbers	100
Mobile Technology—Authentication Service Security	100
Issues in the Design and Implementation of Cryptography Systems	101
Challenges	101
Cryptography Policies	102
Summary	103
Questions and Answers	103
Exercise	105

5. Network Security

Learning Objectives	106
Introduction	106
Why Computer Security and Network Security are Important	107
Network Security Dimensions	108
Network Perimeter Security	109
Intrusion Monitoring and Detection	110
Types of IDS	111
Network-based Intrusion Detection	111
Network Intrusion Detection Model	112
Host-based Intrusion Detection	113
Intrusion Detection Methods	113
Types of Attacks	114
Access Attacks	114
Modification Attacks	114
Denial-of-Service Attacks	115
Repudiation Attacks	115
Firewalls	116
Demilitarized Zone	118
Multiple Zones	119
Most Common Firewalls	121
Firewall Rule Set	122
Firewall Types	122
Choosing the Correct Firewall	124
Firewall Installation and Configuration	124
Firewall Remote Access Configuration	125
Firewall Management	125
Virtual Private Network	126
VPN Types	126
L2TP	128
Need for Virtual Private Networks	131
Authentication of VPN clients	132
Summary	132
Questions and Answers	133
Exercise	136

6. Security Metrics

137–164

Learning Objectives	137
Introduction	137
Measurement Basics	138
Measurement is an Activity	140
Key characteristics of Security Metrics	141
Security Metrics Today	142
Risk	142
Security Risk Assessments Do Not Measure Risk	144
Measurement Slackers and 'Statistical Alchemy'	144
Why Use the Risk Matrix?	145
Few More Concepts	146

Annualized Loss Expectancy	147
Too Many Security Measures?	148
What is the Harm	148
Return on Investment	149
Total Cost of Ownership	150
The Dissatisfying State of Security Metrics: Lessons from Other Industries	150
Reassessing Our Ideas About Security Metrics	153
Thinking Locally	153
Thinking Analytically	153
Thinking Ahead	154
Analysing Security Metrics Data	154
Applied Analysis	154
Exploratory Analysis	155
What Do You Want to Accomplish?	157
How to Identify and Select the Right Metrics	157
Summary	162
Questions and Answers	163
Exercise	
7. Information Security and Laws	165–179
Learning Objectives	165
Introduction	165
Information Security and the Legal Perspective	166
IPR (Intellectual Property Right)	166
Copyright Law	167
Copyright Act, 1957	168
Patent Law	168
Patents Act, 1970	169
Trademark Law in India	170
Data Mining and the Ethical and Legal Issues	171
Computer Ethics	172
Ethical Issues	172
Privacy issues for Data and Software	173
Software for Privacy	174
Issues of Data and Software Privacy	174
Building Security into Software Life cycle	176
Summary	177
Questions and Answers	177
Exercise	177
Appendix	
Bare Act Copyright Act, 1957	178
8. Cyber Crimes and Related Laws	180–195
Learning Objectives	180
Introduction	180
Cyber crimes (cybercrime)	181
Types of Cyber Crimes	182
Cyber Law	184

Laws made to Prevent Cyber Crimes	184
Information Technology Act, 2000	185
Need of Cyber Laws and Cyber Security	187
Implementation and Scope of Cyber Laws in India	188
Summary	190
Questions and Answers	191
Exercise	191
Cyber Law Cases India and Abroad	191
MySpace Catches a Murderer	191
Official Website of Maharashtra Government Hacked	191
Three People Held Guilty in Online Credit Card Scam	192
Appendix	193
<i>Additional Reading and References</i>	196–197
<i>Glossary</i>	198–209