

Contents

Preface.....xv

Acknowledgment..... xvii

Author’s Bio xix

CHAPTER 1 — Understanding Essential Computer Concepts 1

Objectives.....1

1.1 Understanding Computation1

 Conventional Computer Systems1

1.2 Input3

 Understanding Binary Data4

 Conversion from Binary to Decimal9

 Conversion from Decimal to Binary9

 Hexadecimal.....11

 Converting from Hexadecimal to Binary.....13

 Conversion from Binary to Hexadecimal13

 ASCII, EBCDIC and UNICODE.....14

1.3 Processing.....15

 Boolean Algebra, Logic Gates, and Truth Tables15

 Processor Types (32-bit Processors vs 64-bit Processors)19

4	Storage.....	20
	Compression	21
	Lossy Compression	22
	Lossless Compression	23
5	Output.....	24
	Pixels	24
	Color Depth	25
	Color Models	27
	Screen Resolution	28
6	Beyond Conventional Computing	29
	Quantum Computing Is Poised to Change Everything	29
7	A Brief History of Computing Devices	30
8	Conclusion	49
9	Key Words	51

CHAPTER 2 — Cybercrime in a Data-Driven and Techno-Centric Society..... 53

	Objectives.....	53
1	Cybercrime and the Cybercriminal	53
2	The Origin and Definition of Cybercrime – It’s the Data, Always the Data	55
3	Brief Summary of the Phases and Evolution of Cybercrime.....	58
	Phase I.....	60
	Phase II.....	62
	Phase III	63
	Phase IV	67
4	Cybercrime Categories	73
	The Three Cybercrime Categories.....	73
5	The Future of Cybercrime	76
	The Making of the Cybercriminal.....	76
	Cybercrime and the Internet of Things (IoT)	78
	Cybercrime: Machine Learning and Artificial Intelligence.....	79
	Online Child Sexual Abuse and Exploitation (CSAE).....	80
	Cost of Cybercrime.....	81
	The Role of Cryptocurrency in Cybercrime	81
	State-Sponsored Cyberwarfare and Industrial Espionage.....	83
6	Conclusion	84
7	Key Words	85

CHAPTER 3 — Understanding the U.S. Legal System

	Objectives.....	87
	Introduction.....	87

	I. Jurisdiction and Extradition	88
	II. Online Anonymity	89
	III. Digital Evidence	90
	IV. Most Cybercrimes Are not Reported	90
3.2	A Brief Overview of the Legal System in the United States.....	91
	I. The Constitution	92
	II. Statutory or Statute Law	93
	III. Administrative Laws (Agency Regulations) and Ordinance Law	95
	IV. Judicial Decisions or Precedents or Case Law.....	96
	3.2.1 The Courts System	96
3.3	Types of Laws.....	99
	3.3.1 Administrative Law	99
	3.3.2 Civil Law.....	100
	3.3.3 Criminal Law.....	100
3.4	Conclusion	102
3.5	Key Words	104

CHAPTER 4 — Laws, Standards, and Regulations Affecting Cybercrime

	Objectives.....	105
4.1	Introduction.....	105
	4.1.1 Current Legislative Framework in the United States.....	106
4.2	Anti-Hacking Laws	109
	4.2.1 The Federal Computer Fraud and Abuse Act	109
	4.2.1.1 Key Terms and Major Cases to Understand CFAA	112
	4.2.1.2 Limitations of the CFAA	116
	4.2.2 Computer Hacking Laws from Individual States	117
	4.2.3 The Economic Espionage Act of 1996 (EEA).....	117
	4.2.3.1 Important Cases	118
	4.2.4 The Digital Millennium Copyright Act.....	119
	4.2.4.1 Penalties for 17 U.S.C. § 1201	122
	4.2.4.2 Important Cases	123
4.3	Data Security Laws and Regulations in the Private Sector Entities.....	125
	4.3.1 The National Institute of Standards and Technology Cybersecurity Framework	126
	4.3.2 Laws Dealing with Healthcare	128
	4.3.2.1 The Health Insurance Portability and Accountability Act (HIPAA)	128
	4.3.2.2 Penalties for Violating HIPAA Rule	131
	4.3.3 Health Information Technology for Economic and Clinical Health Act	131
	4.3.4 Protecting Consumers’ Privacy Rights with FTC’s Section 5: Federal Trade Commission Act	132

4.3.4.1	Important FTC Cases.....	133
3.5	Laws Affecting Financial Institutions	134
4.3.5.1	The Gramm-Leach-Bliley Act of 1999 (GLBA).....	134
4.3.5.2	Red Flags Rule	137
3.6	Laws Affecting Utilities	138
4.3.6.1	The Federal Energy Regulatory Commission.....	138
4.3.6.2	Nuclear Regulatory Commission.....	140
	Public and Private Sector Entities Partnerships in Cyberspace	140
4.1	Cybersecurity Information Sharing Act of 2015 (CISA)	141
4.2	The Cybersecurity and Infrastructure Security Agency	142
4.3	The National Cybersecurity and Critical Infrastructure Protection Act of 2014 (NCPA)	143
4.4	Cybersecurity Enhancement Act of 2014 (CEA).....	143
	Cybersecurity Requirements for Federal Government Contractors	144
5.1	Federal Information Security Modernization Act of 2014	145
5.2	NIST Information Security Controls for Government Agencies and Contractors	146
	Most Important Internet Surveillance Laws in the United States	147
5.1	All Writs Act	147
4.6.1.1	Significant Case.....	147
5.2	Fourth Amendment	148
4.6.2.1	Search and Seizure	149
4.6.2.2	Exceptions to the Search Warrant Rule.....	150
4.6.2.3	Electronic Surveillance: Private vs Public	151
4.6.2.4	Exclusionary Rule and the Good Faith Exception	153
4.6.2.5	The USA PATRIOT Act and the Fourth Amendment. ...	153
5.3	Electronic Communication Privacy Act of 1986	154
5.4	Communication Assistant for Law Enforcement Act of 1994 (CALEA).....	156
	Key Privacy Laws in the United States.....	157
5.1	Privacy Act of 1974	158
5.2	Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act).....	158
5.3	18 U.S.C. § 1037 Fraud and Related Activity in Connection with Electronic Mail.....	159
5.4	18 U.S.C. § 1029 Fraud and Related Activity in Connection with Access Devices	160
5.5	18 U.S. Code § 1028 Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information	161
5.6	Children's Online Privacy Protection Act of 1998	162
5.7	Video Privacy Protection Act (VPPA) of 1988	164
5.8	When the United States Began Taking Privacy Seriously.....	165

4.8	Conclusion	166
4.9	Key Words	169

CHAPTER 5 — The Networking Environment..... 171

	Objectives.....	171
5.1	Introduction to Computer Networking.....	173
5.1.1	Protocols.....	175
5.1.2	The World Wide Web and the Internet	176
5.1.3	Advantages and Disadvantages.....	178
5.1.4	Essential Computer Network Components and Terminology ...	179
5.1.5	Basic Anatomy of IPv6.....	188
5.1.6	Using Network Utilities	195
5.2	Types of Networks.....	199
5.3	Network Topology.....	202
5.4	The Open Systems Interconnection (OSI) Model.....	206
5.5	The Internet Protocol Suite (TCP/IP).....	210
5.5.1	TCP	212
5.5.2	UDP.....	213
5.6	How Everything Works Together on the Internet: A Review.....	216
5.7	Conclusion	218
5.8	Key Words	219

CHAPTER 6 — Computer Security Technology and Principles..... 221

	Objectives.....	221
6.1	Introduction.....	221
6.2	Understanding Security Terminology	230
6.3	Types of Cyberattacks.....	235
6.3.1	Adware	237
6.3.2	Denial-of-Service Attacks	238
6.3.2.1	Notable DDoS Attacks	245
6.3.2.2	DoS Attacking Tools.....	245
6.3.3	Malware	246
6.3.4	Phishing	248
6.3.5	Spoofing	250
6.3.6	Structured Query Language (SQL) Injection or (SQLI).....	251
6.3.7	Wi-Fi Hacking.....	252
6.4	Prevention Mechanisms.....	256
6.4.1	If You Connect It, Protect It.....	256
6.4.2	Types of Firewalls	259

5 Identification, Authentication, and Authorization.....261

6 Modern Encryption262

6.6.1 Symmetric Encryption or Secret Key Cryptography (SKC)263

6.6.2 Asymmetric Encryption or Public Key Cryptography or
Asymmetric Cryptography266

6.6.3 Digital Certificates and Certificate Authority.....269

6.6.4 Hash Functions or Hashing Algorithms270

What Does “Salting” a Hashtag Mean?272

7 Conclusion273

8 Key Words274

APTER 7 — Internet of Things (IoT)s) 275

bjectives.....275

1 The Internet of Things—An Introduction276

2 A Summary of IoT Applications279

7.2.1 Automotive Sector.....279

7.2.2 Energy Sector.....280

7.2.3 Healthcare Sector281

7.2.4 Manufacturing Sector.....282

7.2.5 Retail Sector.....284

7.2.6 Smart Structures (Buildings, Roads, and Bridges Sector)284

7.2.7 Smart Homes.....285

7.2.8 Transportation Sector.....286

IoT Components, Data Processing Architectures, and Protocols.....286

7.3.1 Basic Components and Data Processing286

7.3.2 Big Data in IoT.....288

7.3.3 Architectures290

7.3.4 Protocols and Standards.....293

Network Consideration for IoT Devices.....299

Security.....301

Conclusion304

Key Words304

PTER 8 — Mobile Devices: The Smartphone. 307

jectives.....307

Introduction.....307

A Brief History and Significant Milestones of Mobile Phones308

Components, Operating Systems (OS), Applications and Architecture .313

8.3.1 Main Components.....313

8.3.2 Operating Systems (OS) and Applications (apps).....316

8.3.3 Platform Architectures.....317

8.4 The Cellular Network322

8.4.1 What Happens When a Mobile Phone Is Turned On?.....325

8.4.2 The Cell Tower or Cellular Base Station.....328

8.4.3 Mobile Device Tracking Location: Cell Towers, GPS, and
Indoor Localization329

8.5 Security.....332

8.5.1 Physical Security333

8.5.2 Executable Security.....335

8.6 Conclusion338

8.7 Key Words340

Appendix A: A Complete Text of the Computer Fraud and Abuse Act
(CFAA) 18 U.S.C. § 1030.....343

Appendix B: 17 U.S.C. § 1201 Circumvention of Copyright Protection
Systems359

Appendix C: HIPAA §164.308 Administrative Safeguards377

Appendix D385

Appendix E: 15 U.S.C.391

Appendix F.....401

Appendix G405

Appendix H411

Appendix I: Valuable IT and Management Certifications415

Index.....419