

BRIEF CONTENTS

Acknowledgments	xxi
Introduction	xxiii

PART I: CORE PRINCIPLES

Chapter 1: What Is Cybersecurity?	3
Chapter 2: The Threat Landscape	19
Chapter 3: Identification and Authentication	29
Chapter 4: Authorization and Access Controls	43
Chapter 5: Auditing and Accountability	61
Chapter 6: Cryptography	73

PART II: ARCHITECTURE, INFRASTRUCTURE, AND SYSTEM SECURITY

Chapter 7: Security Architecture	97
Chapter 8: Network Security	111
Chapter 9: Operating System Security	125
Chapter 10: Mobile, Embedded, and Internet of Things Security	141
Chapter 11: Application Security	157
Chapter 12: AI Security	177

PART III: SECURITY OPERATIONS AND MANAGEMENT

Chapter 13: SecOps, the SOC, and Incident Response	195
Chapter 14: Governance, Risk, and Compliance	209
Chapter 15: Vulnerability Assessments and Penetration Testing	229

PART IV: HUMAN FACTORS AND PROFESSIONAL DEVELOPMENT

Chapter 16: Social Engineering	249
Chapter 17: Security Awareness	263
Chapter 18: So You Want to Be a Security Professional	277
Notes	289
Index	297