Cybersecurity Risk Assessments

Steven M. Bragg

Table of Contents

Chapter 1 – Cyber Risk in the Business Context 1
Learning Objectives 1
Introduction 1
The Business Context for Cyber Risk 2
Core Cybersecurity Concepts and Terminology 5
Oversight of Cyber Risk 7
Regulatory, Legal, and Contractual Considerations 11
Review Questions 15
Review Answers 16

Chapter 2 – Assessment Methodologies and Scoping 19
Learning Objectives 19
Cybersecurity Risk Assessment Methodologies 19
Establishing the Scope of the Assessment 22
Review Questions 26
Review Answers 27

Chapter 3 – Assets, Threats and Vulnerabilities 29
Learning Objectives 29
Asset Identification and Classification 29
Understanding the Threat Landscape 34
Vulnerability Identification 38
Review Questions 43
Review Answers 44

Chapter 4 – Analyzing Risk and Evaluating Controls 45
Learning Objectives 45
Risk Identification and Scenario Development 45
Assessing Likelihood and Impact 49
Evaluating Existing Controls 54
Review Questions 59
Review Answers 60

Chapter 5 – Technology and Third-Party Risk Domains 61
Learning Objectives 61
Identity and Access Management Risks 61
Data Protection and Privacy Risks 64
Infrastructure, Network, and Endpoint Risks 67
Cloud, SaaS, and Emerging Technology Risks 70
Third-Party and Supply Chain Cyber Risks 73
Human Factors and Security Awareness Risks 76
Review Questions 80
Review Answers 81

Chapter 6 – Resilience and Business Consequences 83
Learning Objectives 83
Business Resilience 83
Fraud, Financial Reporting, and Operational Risks from Cyber Events 87
Review Questions 90
Review Answers 91

Chapter 7 – Prioritizing, Treating, and Reporting 93
Learning Objectives 93
Risk Prioritization 93
Risk Treatment Strategies 96

Reporting Cyber Risk Assessment Results 99
Monitoring and Reassessment 102
Common Weaknesses in Cyber Risk Assessments 105
Summary 108
Review Questions 109
Review Answers 110

Glossary 113

Index 115