Table of Contents

About the Authors xi

Series Editor's Foreword xiii

Foreword xix

Acknowledgments xxi

Chapter 1: What Are We Afraid Of? 1

Understanding the Threat Environment 1

Overview of the Risk Landscape 2

Understanding the Adversary 3

Threat Categories for Financial Organizations 6

That's Where the Money Is–Theft of Funds 6

Information Is Power–Theft of Data 7

Clogging Up the Works–Threats of Disruption 9

Facing the Threats 11

Threat Intelligence 12

Threat Modeling 13

Implementation 15

Moving Ahead 17

Notes 18

Chapter 2: Where Are We Vulnerable? **21**
Cybersecurity Weaknesses 21
Technology Vulnerabilities 22
New Technologies 27
Human Vulnerability Dimensions 29
An Illustration: Business E-mail Compromise 32
Understanding the Consequences 34
Moving Ahead 46
Notes 46

Chapter 3: What Would a Breach Cost Us? **49**
Risk Quantification 49
Scenario Creation 54
Scenario Selection 58
Cost Estimation 62
Moving Ahead 70
Notes 70

Chapter 4: What Are the Odds? **73**
Plausible Deniability 73
Cybersecurity Risk As Operational Risk 75
Shortage of Sufficient Historical Data 78
Probabilities Driven by Vulnerabilities 82
The Next Evolution 91
Moving Ahead 100
Notes 101

Chapter 5: What Can We Do? **105**
Risk Treatment Across the Organization 106
Avoidance 106
Reduction 107
Transfer 111
Acceptance 114
Risk Treatment Across the Enterprise Architecture 115
Executing on Risk Treatment Decisions 118
Validating Effectiveness in Execution 121
Moving Ahead 123
Notes 124

Chapter 6: How Do I Manage This? **125**
Governance Operating Model 126
Cybersecurity Risk Appetite 133
Cybersecurity Performance Objectives 140
Moving Ahead 154
Notes 154

Chapter 7: Should This Involve the Whole Organization? **157**
Architectural View 158
Enterprise Capabilities 168
Monitoring and Reporting 176
Metrics 184
Moving Ahead 189
Notes 190

Chapter 8: How Can We Improve Our Capabilities? 193

Build a Learning Organization 194

Improve the Quality of Risk Assessments 197

Use Organizational Knowledge 203

Take Action Based on the Risk Assessment 205

Build Situational Awareness 207

Conduct Realistic Drills, Tests, and Games 211

Design of Technical Tests 215

Move from Controls-Thinking to Capabilities-Thinking 217

Moving Ahead 219

Notes 220

Chapter 9: What Can We Learn From Losses? 223

Breaches Provide the Context That Standards Lack 224

Technology-Focused Resilience Is Just the Beginning 225

The Learning Organization Revisited 226

Easier Said Than Done 227

AntiFragile 228

Learn, Study Mistakes, and Learn Again 231

Moving Ahead 232

Notes 233

Chapter 10: So What's Next? 235

Complexity and Interconnectedness 235

Potential Cybersecurity Implications 240

Emerging Standards 243

Notes 248

Index 251