

Table of Contents

About the Authorix

About the Technical Reviewerxi

Acknowledgmentsxiii

Foreword 1xv

Foreword 2xix

Introductionxxiii

Part I: The Problem..... 1

Chapter 1: What Is the Problem?3

 Introduction..... 3

Chapter 2: Why Is It Complicated?7

 Introduction..... 7

 Technology Is Everywhere 8

 Technology Is Complex..... 9

 Technology Was Built on Trust..... 10

 Technology Is an Opportunity for Misuse 11

 The Fundamental Risk Is Not Always Understood..... 12

 ... and Business Leaders Need to Know What to Do 13

 Keep in Mind 14

 Lack of a Common Cybersecurity Risk Language..... 15

TABLE OF CONTENTS

Unclear Answers for Proper Oversight..... 17

Oh, and Umm... Distractors..... 18

Chapter 3: How to Address This Problem21

Introduction..... 21

Understand the Risk..... 22

Manage the Risk 25

Apply a Framework..... 25

Structure the Organization..... 27

Set a Review Frequency 27

Prepare to Respond (and Recover) 28

Measure the Impact of Risk Management..... 28

Keep in Mind 28

Choose Risk-Informative Measures 29

Apply Appropriate Resources..... 30

Drive for Value..... 30

Be Clear on What to Measure..... 31

Avoid Chasing “Perfect” (It’s Not That Valuable) 32

Part II: The Solution 33

Chapter 4: Understanding the Problem35

Introduction..... 35

Rules to Follow..... 37

Be Clear About the Problem (Critical Assets Are at Risk) 37

Settle on a Definition of *Risk*..... 38

Settle on a Definition of *Critical* 40

Inventory and Categorize Critical Assets..... 44

How to Inventory and Categorize Critical Assets 45

TABLE OF CONTENTS

Step 1. Acknowledge That Asset Management Is Hard.....	46
Keep in Mind	46
Step 2. Develop the Business Case.....	47
Step 3. Define Your Asset Classes.....	48
Step 4. Collect and Inventory in Each New Asset Class	50
Step 5. Identify the Most Critical Assets	51
Identify the Risks to These Critical Assets	53
How to Identify the Risks to These Critical Assets	53
Step 5a. Perform a Threat Analysis.....	54
How to Walk Through an Overview of a Threat Model	56
Step 5b. Discover Vulnerabilities.....	57
Step 5c. Anticipate the Business Impact of an Event.....	60
Step 5d. Pull It Together in the Risk Register and Keep It Updated	63
Step 5e. Know the Applicable Laws and Regulations	64
Step 5f. Connect Cybersecurity Risk to Enterprise Risk.....	66
Understanding the Problem: A Recap	69
Recent Examples	69
Example 1. Getting Started with a Program.....	70
Example 2. From Legacy “Perfection” to “Good Enough”	76
Example 3. Data Protection Strategy, Please	79
Example 4. What Risk?	82
Pitfalls to Avoid	83
Chapter 5: Manage the Problem	85
Introduction.....	85
General Observations and Guidelines for Managing the Risk	87
Observations	87
Guidelines	88

TABLE OF CONTENTS

Rules to Follow.....90

Focus on One Framework90

Structure the Program Approach95

How to Structure the Approach.....96

Step 1. Set the Structure97

Step 2. Align the Risk-Mitigating Activities99

Step 3. Assign Roles and Responsibilities100

Step 4. Identify Gaps and the Appropriate Activities to Fill Them103

Step 5. Look Externally (Third-Party Risk Management)105

How to Build Out the TPRM Questionnaire107

Step 5a. Split the Questionnaire into Logical Columns108

Step 5b. Build Each Column Upon the One Before108

Step 5c. Directly Relate the Question to the Risk.....108

Keep in Mind110

How to Verify Your External Look113

Step 5d. Link a Software Bill of Materials to the TPRM Program.....113

Step 5e. Build a Feedback Mechanism for Vendors.....116

Step 5f. Align to Procurement and Purchasing117

Keep in Mind: Third-Party Risk Management.....119

Step 6. Pick the Right Tools and Avoid Distraction.....120

Set a Program Review Frequency.....123

Prepare to Respond and Recover.....125

Managing the Problem, a Recap125

Recent Examples126

Example 1. Addressing Too Many Frameworks.....126

Example 2. Many TPRM Tools130

Example 3. From Controls Focus to a Risk Strategy133

Example 4. Third-Party Without a Checklist..... 136

Pitfalls to Avoid 138

Chapter 6: Get Ready for Measures141

 Introduction..... 141

 Keep in Mind: Consider the Broad View of Risk for Measurement..... 143

Chapter 7: Measure the Problem145

 Introduction..... 145

 Rules to Follow..... 146

 Choose Informative Measures That Provide Actionable Values..... 147

 How to Choose Informative Measures 149

 Step 1. Choose Actionable Measures..... 149

 Step 2. Define Clear Addressable Activities 150

 Step 3. Provide Actionable Reviews..... 151

 Research What Others Have Done (Measures That Have Worked)..... 152

 Measures That Have Worked..... 153

 Be Clear About the Math 154

 Straight Math 154

 Less-Than-Straight Math 156

 Gain Buy-In from Stakeholders 157

 Develop a Reporting Structure for Consistency 159

 Allow Measures to Mature Over Time 161

 Keep in Mind: Consider the Insights 162

 Recent Examples 163

 Example 1. Simple Measures, Anyone? 163

 Example 2. Too Much Data, Not Enough Information 169

 Pitfalls to Avoid 172

TABLE OF CONTENTS

Chapter 8: Report Upward175

 Introduction..... 175

 Rules to Follow..... 176

 Rules to Follow: Report Upward..... 177

 Choose a Consistent Reporting Structure 177

 Provide Clear and Informative Measures 179

 Keep in Mind: Consider the Value..... 180

 Use Straightforward Terms 181

 Provide Recommendations for All Problems 182

 Pitfalls to Avoid 182

Chapter 9: Questions Boards Should Ask185

 Introduction..... 185

 A Tear Sheet for Boards 192

Chapter 10: Conclusion.....195

 Introduction..... 195

 First, Understand the Risk..... 195

 Next, Manage the Risk 201

 Then, Measure the Risk 204

 Go Forth and Prosper 208

Appendix: Illustration209

Index.....217