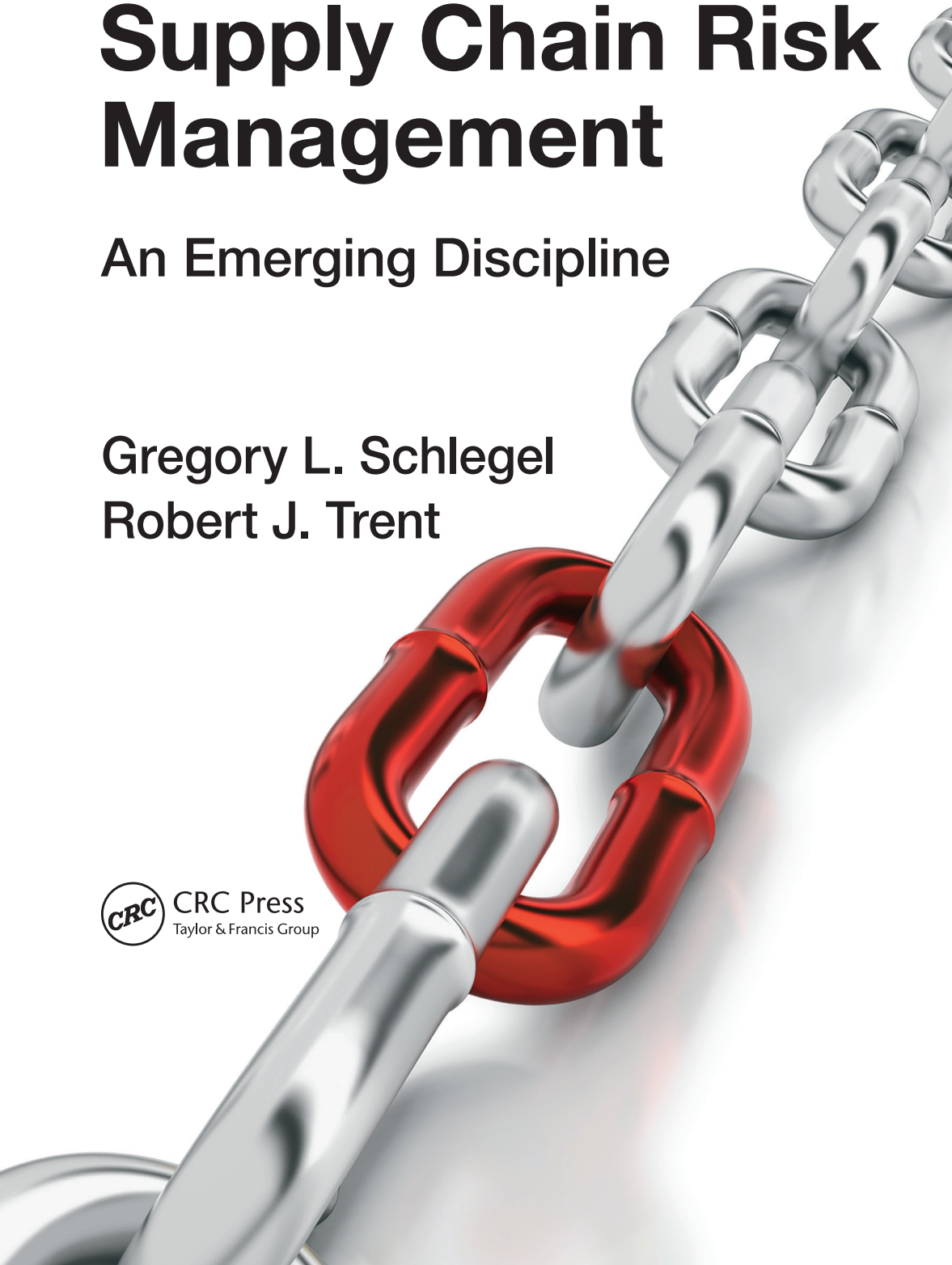
Series on Resource Management

Supply Chain Risk Management

An Emerging Discipline

Gregory L. Schlegel
Robert J. Trent



CRC Press
Taylor & Francis Group

Supply Chain Risk Management

An Emerging Discipline

Supply Chain Risk Management

An Emerging Discipline

Gregory L. Schlegel
Robert J. Trent

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20160321

International Standard Book Number-13: 978-1-4822-0599-2 (eBook - PDF)

Contents

Preface xiii
About the Authors xix

Chapter 1 Supply Chain Risk Management: Setting the Stage 1

The Concept of Risk and Risk Management 2
Defining Enterprise Risk Management 3
Defining Supply Chain Risk Management 6
Why Focus on Supply Chain Risk Management? 7
Some SCRM Observations 10
Why Aren't We Prepared for SCRM? 10
Some Important Risk Concepts 11
Risk Event 11
Risk Exposure and Vulnerability 12
Risk Resilience 13
Risk Appetite 14
Risk Analysis or Assessment 15
Risk Response Plan 15
Risk Compliance 15
Risk Governance 16
Categorizing Risk 16
Other Ways to Look at Risk 17
Generic Risk Management Approaches 18
Risk Mitigation 18
Risk Avoidance 19
Risk Prevention 19
Risk Acceptance 20
Risk Sharing 20
Prevention versus Responsiveness 21
Concluding Thoughts 21
Summary of Key Points 21
Endnotes 22

Chapter 2 Supply Chain Risk Management: The As-Is Landscape ... 25

A Chronology of Supply Chain Risk Management 25
2009 26
2010 27
2011 30
2012 32
2013 34
Four Pillars of Supply Chain Risk Management 36
Supply Risk 37
Process Risk 37
Demand Risk 37
Environmental Risk 37
The Supply Chain Risk Management Adoption 39
SCRM Adoption 40
Concluding Thoughts 41
Summary of Key Points 42
Endnotes 43

Chapter 3 Building the Risk Management Foundation 45

Supply Chain Risk Management Enablers 45
A Supportive Organizational Design 46
Information Technology 51
Measurement Systems 53
Talent Management 54
Linking Supply Chain Risk Management and Supply Chain Strategy 56
Integrating Risk Management with Commodity Strategy Development 57
The Ultimate Risk—Improve or Else! 59
Rallying around a Superordinate Measure 60
Reducing Supply Risk through a New Approach to Contracting 61
Systems Contracting Benefits 62
Concluding Thoughts 63
Summary of Key Chapter Points 64
Endnotes 65

Chapter 4 Strategic Risk 67

What Is Strategic Risk? 68
Reducing Strategic Risk through Better Product Development 69
New Product Development Best Practices 69
Bringing New Product Development and Risk Management Together 73
The Art and Science of Not Getting Caught by Surprise 74
Protecting Intellectual Property 79
When Strategic Risk Becomes Strategic Reality 82
Concluding Thoughts 84
Summary of Key Points 85
Endnotes 86

Chapter 5 Hazard Risk 87

The Traditional World of Hazard Risk and Insurance 87
First-Party Commercial Property Insurance 89
Cargo Insurance 90
Cyber Insurance 90
Business Interruption Insurance 90
Contingent Business Interruption Insurance 91
Trade Disruption Insurance 91
Global Logistics Insurance 92
Quantifying Traditional Hazard Risk Insurance Requirements 94
Looking at the Thai Floods through a Risk Quantification Prism 100
Concluding Thoughts 101
Summary of Key Points 102
Endnotes 102

Chapter 6 Financial Risk 103

Understanding Financial Risk 104
Supplier and Customer Financial Viability 104
Supply Market Volatility 105
A Case Study of Supply Market Volatility 106

Getting Serious about Managing Financial Risk.....107
Supplier Financial Health Assessment through Ratio Analysis 108
Bankruptcy Predictors.....111
Private Company 112
Public Company.....112
Qualitative Supplier Financial Risk Indicators 115
Assessment of Customer Creditworthiness.....116
Hedging.....118
Currency Risk Management Approaches 120
Concluding Thoughts 123
Summary of Key Points 124
Endnotes 124

Chapter 7 Operational Risk 127

Operational Risks.....127
Supply Risk 128
Demand Risk.....131
Process Risk..... 134
Environment/Ecosystems Risk.....137
Business Continuity Planning.....139
Business Continuity Planning Objective 140
The Business Continuity Life Cycle 141
BCP Exercises.....144
Concluding Thoughts 145
Summary of Key Points 145
Endnotes 146

Chapter 8 Supply Chain Fraud, Corruption, Counterfeiting, and Theft 147

Some Key Concepts.....148
Bribery.....148
Counterfeiting.....149
Fraudulent, Corrupt, Coercive, and Collusive Practices ...150
Rules and Regulations 153
Consumer Financial Protection Bureau (CFPB).....153
Customs Trade Partnership against Terrorism (C-TPAT)..... 154

Dodd-Frank Wall Street Reform and Consumer Protection Act 155
Foreign Corrupt Practices Act 155
Tools, Best-in-Class Practices, and Countermeasures 156
Fraud, Corruption, and Theft Tools 156
Supplier Co-Management 158
Addressing Corruption with Best Practices 159
Counterfeit Countermeasures 161
Concluding Thoughts 162
Summary of Key Points 163
Endnotes 163

Chapter 9 Emerging Risk Management Frameworks for Success ... 165

What Is a Framework? 165
Frameworks Supporting the New Supply Chain Risk Management Discipline 166
Enterprise Risk Management (ERM) Framework 166
COSO ERM Framework 167
ISO Standards 168
Governance, Risk, and Compliance (GRC) 172
Risk Taxonomies—An Operational Framework For SCRM 175
Leveraging ERM, GRC, and Risk Taxonomies 177
Benefits of ERM and GRC Frameworks 180
Concluding Thoughts 183
Summary of Key Points 183
Endnotes 184

Chapter 10 Using Probabilistic Models to Understand Risk 185

Defining the Models 185
Probabilistic versus Deterministic Modeling Tools 187
Risk Response Plans 191
Company Examples of Probabilistic Modeling 192
Scenario Planning at DuPont 192
Stress Testing the Supply Chain at Bayer Material Sciences 194
Next-Generation S&OP at Huntsman 197

Concluding Thoughts 200
Summary of Key Points 200
Endnotes 201

Chapter 11 Using Big Data and Analytics to Manage Risk 203

What Is Big Data and Predictive Analytics, Really? 204
The Process of Successfully Leveraging Big Data for Maximum Benefit 207
Barriers and Challenges Moving Forward 209
Tools, Techniques, and Methodologies Supporting Big Data 210
How Early Adopter Companies Leverage Big Data 213
Consumer Packaged Goods 214
Dell Computers 214
Western Digital 215
Harley Davidson 215
Raytheon 216
European Electrical Utility 216
Schneider 217
Concluding Thoughts 218
Summary of Key Points 219
Endnotes 219

Chapter 12 Emerging Risk Management Tools, Techniques, and Approaches 221

Become a Preferred Customer 221
Gaining Preferred Customer Status 223
Construct Supply Chain Heat Maps 225
Map the Supply Chain 226
Challenges When Mapping a Supply Chain 226
Supply Chain Mapping Guidelines 227
Decluster the Clusters 229
Clustering Gone Wild 230
Create a Flexible Supply Chain 231
Examples of Flexibility 232
Create a Risk War Room 237

Manage Working Capital 238
Controlling Inventory through Perfect Record Integrity 239
Effective Demand Estimation and Management 240
Concluding Thoughts 242
Summary of Key Chapter Points 242
Endnotes 243

Chapter 13 Risk Measurement 245

Risk Measurement Validity and Reliability 245
Validity and Bridge Safety Measures 247
Supplier Performance Measurement—Doing It Right 248
Quantified Risk Indexes 250
A Risk Index Example 251
Country Risk Indexes 251
Using Total Cost Measures to Manage Risk 252
Types of Total Cost Models 253
Supplier Capacity Estimate Measures 258
Emerging Supply Chain Risk Metrics 260
Value at Risk 260
Time-to-Recovery 260
Risk Exposure Index 261
Supply Chain Key Performance Indicators 261
Concluding Thoughts 264
Summary of Key Points 264
Endnotes 265

Chapter 14 Learning from Risk Management Leaders 267

Making Risk Management a Priority at Boston Scientific 267
Having the Right Tools 268
Navigating Threats at Boeing 269
Supplier Risk Assessment at IBM 271
IBM's Risk Management Tool 272
Using Supply Chain Mapping to Manage Risk at Cisco 274
Surviving a Near-Death Experience at Delphi 275

Managing Strategic Risk through Collaborative Cost Management....276
A Collaborative Approach to Cost Management..... 277
Learning about Risk the Hard Way at J. C. Penney.....279
Concluding Thoughts 280
Endnotes 281

Chapter 15 Future Directions in Supply Chain Risk Management ... 283

Supply Chain Risk Management Predictions..... 283
An Evolving Risk Management Maturity Model 291
Supply Chain Risk Maturity Model..... 292
Visibility..... 292
Predictability.....293
Resiliency.....293
Sustainability..... 294
A Call to Action..... 294
Establish the Risk Leadership Team 294
Establish Risk Crisis Teams.....295
Focus on the Risk-Management Enablers..... 296
Assess the Current State of Risk Management Preparedness 296
Perform Risk Assessments and Develop Risk Management and Business Continuity Plans..... 297
Gain Visibility across the Supply Chain..... 297
Benchmark Risk Management Practices against Industry Leaders..... 298
Develop or Obtain the Tools, Techniques, and Risk Protocols 298
Concluding Thoughts 298
Endnotes..... 299

Appendix: The Supply Chain Risk Assessment Tool 301
How You Might Utilize the Tool.....301
Walking through the Questions-of-Discovery 303
How to Access the Tool 303

Preface

Perhaps the best way to introduce a book about supply chain risk management (SCRM) is to start with some real although not necessarily uplifting stories. Each of the following occurred in the same week and year during a December holiday season. The names of the companies involved have not been changed to protect the innocent.

Guaranteed On-Time Delivery, Except When It's Not. In its end-of-year edition, *Business Week* magazine prominently featured a cover story about how UPS was going to save Christmas. The magazine chronicled the efforts of the man responsible for making sure all those packages ordered just before Christmas would make their way under the tree in time. Retailers such as Amazon guaranteed that orders placed by December 23 would arrive in time for the big day. This was going to be a defining moment for supply chain managers and online retailers! A convergence of events, however, ensured that Scrooge would have the final say.

What actually happened is a perfect storm that will be studied for many years. While big shippers like Amazon claimed their innocence by announcing that its shipments were given to UPS on time (failures from risk events almost always feature blaming someone else), not enough planes at UPS were available to move such a large number of packages, creating huge bottlenecks.

So, what happened? More consumers than forecast shopped online that holiday season, creating higher-than-anticipated demand. And, only 26 days separated Thanksgiving and Christmas, compared with 32 days the previous year. A great deal of shopping was crammed into fewer shopping days. It did not help that bad weather across much of the United States during this period interrupted package delivery service. Bad weather had a secondary effect of keeping consumers inside where they proceeded to do to even more online shopping. And not surprisingly, many consumers waited until the last minute to place their orders. Why not wait? Retailers such as Amazon guaranteed delivery even though UPS has some fine print stating that delivery is not guaranteed during peak holiday periods. Unfortunately, UPS took a substantial hit to its earnings and reputation.

When Swiping Means Getting Swiped. Target Corp. announced that 40 million customer credit cards were in jeopardy because of a security

breach at its point-of-sale store registers. A few days later Target admitted that personal data for up to 70 million customers was also compromised. The retailer told customers they should examine transactions made on their credit and debit cards during a 19-day period and report any fraudulent sales. Making matters worse, credit and debit card accounts stolen during this period reportedly flooded underground black markets, going on sale in batches of one million cards. A fraud analyst at a major bank said his team purchased a portion of the customer accounts from an online store advertised in cybercrime forums. The reporting of this security breach coincided with a subsequent drop in Target's sales, likely due to a loss in customer confidence.

Shortly after the security breach Target, executives announced a set of actions that cost some serious money

Target closed the access point that the criminals used and removed the malware they left behind; hired a team of security experts to investigate the security breach; communicated that its customers would have zero liability for any fraudulent charges arising from the breach; and offered one year of free credit monitoring and identify theft protection to all customers. It's no fun getting swiped.

Heavy Metal Hoarders. A report in *The Wall Street Journal* revealed that banks, hedge funds, commodity merchants, and other investors were hoarding tens of millions of tons of aluminum, copper, nickel, and zinc in a system of hidden warehouses around the world. So what's the big deal? Once hidden in these warehouses, these metals are no longer tracked, making accurate calculations of market supply, something that is needed to determine commodity prices, next to impossible to determine. Producers are bracing for wild swings in metals' prices as speculators withhold data to take advantage of pricing volatility. Market manipulation is likely as metals are controlled by fewer and fewer hands whose interests are likely not aligned with legitimate commodity users.[1]

Toss This Example. In an unfortunate case of how the Internet and social media can place a company's reputation at risk in the blink of an eye, a home security video system captured a FedEx driver tossing a package onto a customer's porch. This might have remained a local event except for the fact that millions of people watched the uploaded video as it went viral. Judging from the driver's throwing technique he is likely the star of his Frisbee golf team.

Welcome to the world of supply chain risk management. It is a world where the end of your day might not be nearly as good as the start of your

day. While the examples presented here caused problems at many levels, and we do not want to diminish the harm that came to innocent bystanders, they illustrate that what can happen in a typical week is not always all that typical. As we will discuss, the supply chain world is becoming riskier rather than safer. A survey used to calculate the Allianz Risk Barometer recently concluded for the first time that supply chain risk is now the top concern of global insurance providers. This reinforces our belief that a book about supply chain risk management is relevant and timely. So, how was your week?

SUPPLY CHAIN RISK MANAGEMENT THEMES

As we progress through this book, certain themes are revealed that underlie our view of supply chain risk management. These themes support the basis for everything we present.

- **The financial impact of supply chain disruptions can be devastating but is often not understood until it is too late**. Studies show that, on average, if a publicly held company experiences a moderate or higher risk event, it can expect a 7%–10% reduction in shareholder value. And, approximately 30% of companies that experience a major risk event are out of business within 24 months of the event, and another 25% are out of business after three years.
- **The supply chain management profession has become too comfortable with the deterministic models and tools developed over the last 35 years.** The relatively stable environment of the last 35 years is no longer in existence, and deterministic tools such as forecasting models and sales and operations planning (S&OP) processes have never taken uncertainty into account. Unfortunately, global supply chain growth has resulted in uncertainty, complexity, and risk growing in frequency and severity. The time has come to utilize probabilistic tools that take into account uncertainty in order to manage risk.
- **SCRM is an evolving discipline and will remain so for the foreseeable future.** To be successful in a new global environment, becoming a risk management leader demands mastering four stages of SCRM excellence: visibility, predictability, resiliency, and sustainability. These are part of something we call the 21st Century Supply Chain Risk Maturity Model.

- **Supply chain strategies driven primarily by cost management and delivery improvements are no longer comprehensive enough.** The time has come to make supply chain risk assessments part of the supply chain planning process. Today these risk assessments are still unfortunately more of an afterthought.
- **Showing a hard return on investment for risk management initiatives is a difficult sell.** How do you justify an investment for managing something as vague as a potential risk event? Our view is that traditional financial models are proving to be inadequate when evaluating risk management investments.
- **Social media is the new risk wild card.** A brand built over 50 years can come under attack with a tweet (regardless of whether the tweet is true or not). A negative video on YouTube can go viral in minutes. Social media can amplify the outcome from risk events that may have previously been localized.
- **The risk ledger has two sides**. One side of the risk ledger is the negative side of risk. The other side of the ledger, however, represents opportunity management. It is the upside of risk, as someone's risk is often another's opportunity. Our focus, while recognizing both sides of this ledger, will stress the downside of risk.
- **Supply chain risk is making it to the big leagues.** Companies are placing supply chain risk management verbiage in their 10K and annual reports, something that was rare not too long ago. This illustrates how seriously supply chain risk is being taken at the corporate level. Unfortunately, it also shows how serious the impact can be from supply chain disruptions.
- **Risk heroics must give way to risk prevention wherever possible**. Interviews with leading executives lead us to a clear conclusion. Most companies are tired of responding, sometimes heroically, when a risk event occurs. Increasingly these companies would like to model, anticipate, and even prevent risk events from occurring. The pendulum needs to shift from heroic responsiveness to proactive risk prevention wherever possible. Constantly running around with your hair on fire gets tiring.
- **We need to take a broader rather than narrower view of supply chain risk management.** As a concept, SCRM is similar to Lean and Six Sigma. A narrow view of these concepts considers them mainly as a set of tools and techniques. The broader view, and the one endorsed throughput this book, is that SCRM, like Lean and Six

Sigma, is supply chain–wide, affects an organization's culture, and can have a positive or negative strategic impact.

- **Supply chain risk is increasing, not decreasing.** With globalization expanding at a remarkable rate over the last 20 years, supply chains have moved into areas where they've never operated. Thus, uncertainty, complexity, and risk have grown exponentially. If anyone claims that supply chain risk is decreasing in terms of impact and concern, ask to see their evidence. We will show an abundance of evidence to indicate the contrary.

ORGANIZATION OF THIS BOOK

This book is organized into four sections. The first section sets the stage by positioning our understanding of supply chain risk management. Chapter 1 explains the important concepts and terminology that appear throughout this book. The second chapter provides an overview of the "as is" state of SCRM, an overview that reveals that while most managers appreciate the importance and danger of risk, few organizations are prepared for this new environment. Chapter 3 recognizes that achieving excellence in any area, including risk management, does not happen simply because a company announces its desire for excellence. It also highlights a set of enablers that provide the foundation for effective risk management.

The second section of this book presents a traditional but still important view of SCRM. Here, we address strategic risk (Chapter 4), hazard risk (Chapter 5), financial risk (Chapter 6), and operational risk (Chapter 7). These chapters will describe many approaches for addressing risk within these four categories.

Section III dives into the emerging discipline called supply chain risk management. Chapter 8 addresses fraud, corruption, theft, and counterfeiting; while Chapter 9 presents a set of emerging risk management frameworks. This is followed by two leading-edge topics—using probabilistic models to understand risk (Chapter 10), and using analytics to predict the future (Chapter 11). Chapter 12 presents an emerging set of risk management tools, techniques, and approaches that are broader than what we typically associate currently with risk management. The important topic of risk measurement appears in Chapter 13, and Chapter 14 presents an overview of companies that are well respected in terms of their risk

management capabilities. The final section of the book consists of a single chapter that provides a forward-looking perspective in terms of SCRM. This chapter also includes a set of steps for moving a company's risk management agenda forward.

This book also includes an appendix, which presents a risk self-assessment tool that will provide value far beyond the cost of this book. We also provide a web address for free access to this tool.

Although this book is not a novel, we recommend reading the chapters in the sequence they are presented. Rest assured, however, that moving out of sequence will not get anyone in too much trouble.

CONCLUDING THOUGHTS

As we proceed, it is important to keep in mind that risk management capabilities are often relative, which the following narrative illustrates: The CEOs of two competing companies are walking through the woods when they come upon a very large and ornery bear. As the bear roars menacingly, one CEO drops quickly to his knee and begins to tighten his shoelaces. The other CEO says, "What are you doing? You can't outrun that bear!" The first CEO replies, "I don't have to outrun that bear. I only have to outrun you!"

Often in business we only have to run a bit faster than our competitors. The same is true in risk management. While we would always like to anticipate and then prevent risk from happening, when risk events do occur, being faster, flexible, and more responsive than others can make a world of difference. A primary objective of this book is to understand within the domain of supply chain risk management how to run a bit faster and better than the others. Let the journey begin!

ENDNOTE

1. Shumsky, Tatyana. "Heavy Metal Lurks in the Shadows." *The Wall Street Journal*, December 27, 2013: C1.

About the Authors

Greg L. Schlegel, CPIM, CSP, JONAH is the vice president of business development for Shertrack LLC. He has been a supply chain executive for more than 30 years with several Fortune 100 companies and spent seven years as an IBM supply chain executive consultant. Greg was APICS' 1997 International Society President. He is well published and a frequent speaker at conferences, seminars, webinars, and dinner meetings.

Greg has taught operations management at the University of Scranton and has been guest lecturer at Arizona State University, St. Johns University, and Rutgers University. He is presently a member of the Business Analytics Roundtable for Villanova University, a member of the board of advisors for Rutgers University's supply chain undergraduate program, and executive in residence for Lehigh University's Center for Value Chain Research. Greg has taught graduate level supply chain risk management at Lehigh University and has been facilitating supply chain risk management public workshops and the new APICS-supported Supply Chain Risk Certificate workshops around the globe for over three years. He is founder of the Supply Chain Risk Consortium, a group of 13 companies providing education, assessment tools, and consulting services in support of supply chain risk management projects. He teaches enterprise risk management at Villanova in their Executive MBA program. Greg is certified CPIM, CSP in systems, and a Theory of Constraints–certified JONAH. He holds a BS in operations research and computer science from Penn State University and did his graduate work at Lake Forest College.

Greg presently lives in Flemington, New Jersey, with his wife Mariann. He can be reached at schlegel01@earthlink.net.

Robert J. Trent, PhD is the supply chain management program director at Lehigh University. He holds a BS degree in materials logistics management from Michigan State University, an MBA degree from Wayne State University, and a PhD in purchasing/operations management from Michigan State University.

Prior to his return to academia, Bob worked for the Chrysler Corporation. His industrial experience includes assignments in production scheduling,

packaging engineering with responsibility for new part packaging setup and the purchase of nonproductive materials, distribution planning, and operations management at a regional parts distribution facility. He has also worked on numerous special industry projects. Bob stays active with industry through research projects, consulting, and training services. He has consulted with or provided training services to 40 government agencies and corporations and worked directly with companies on dozens of research visits.

Bob has authored or co-authored six books and dozens of articles appearing in a range of business publications. He has also co-authored five major research studies published by CAPS Research and has made presentations at numerous conferences and seminars.

Bob and his family reside in Lopatcong Township, New Jersey. He can be reached at rjt2@lehigh.edu.

1

Supply Chain Risk Management Setting the Stage

Floods, earthquakes, tsunamis, tornadoes, and billowing clouds of ash from obscure volcanoes all share something in common. Over the last several years these events have been featured prominently in the news—and each has had the inevitable effect of disrupting the supply chains of entire industries. But these kinds of disruptions were not on the minds of Astellas Pharma executives when thieves stole a trailer from a truck stop containing $10 million of the company's pharmaceutical products. What followed was a lesson in supply chain risk that felt like a swift punch in the gut.

When the accountants had completed their final tabulations, they found that the stolen products represented only a fraction of the losses suffered by Astellas. Based on a recommendation from the U.S. Food and Drug Administration, the company contacted every party in its supply chain, ranging from wholesalers to hospitals, warning them of the stolen drugs. As a preventive measure the company withdrew from the marketplace all drugs with the same lot numbers as those that were stolen. Some of the stolen pharmaceuticals required strict climate control, something the thieves (who were eventually caught) were not too concerned about, making a return of these products a necessity. The loss of this trailer eventually cost the company $47 million, wiping out a large chunk of its North American profit for that quarter.[1]

Welcome to the sometimes unpleasant world of supply chain risk management. This chapter starts our journey into this evolving discipline by setting the stage for important concepts that appear throughout this book. We begin by providing various definitions and perspectives of this thing called *risk*. Next, we present reasons why a focus on supply chain risk management has become a necessity rather than a luxury. This is followed

by an explanation of various risk terms and concepts, a categorization of risk, and a presentation of generic risk management approaches.

THE CONCEPT OF RISK AND RISK MANAGEMENT

A logical place to start is to explain what we mean by risk, particularly since this concept can be defined in various ways. One common perspective simply says that risk is a situation involving exposure to danger or loss. Another perspective takes this a step further by adding that risk is the probability or threat of damage, injury, liability, loss, or other negative occurrences that are caused by external or internal vulnerabilities and that may be avoided through preemptive action.[2] Another view states that risk is the effect of uncertainty on objectives. Risk can also be viewed, at least partly, as the inability to capitalize on an opportunity. For our purposes we define risk as the probability of realizing an unintended or unwanted consequence that leads to an undesirable outcome such as loss, injury, harm, or missed opportunity. Warren Buffet once observed that risk comes from not knowing what you are doing.

Most risk observers believe that when a risk becomes a reality, something bad usually happens. Not surprisingly, supply chain managers almost always look at risk in terms of something to be avoided. And to say that most supply chain managers are generally risk averse would be an understatement. Conversely, entrepreneurs look at risk through a different lens. They view risk in terms of upside opportunities and missed opportunities when failing to act. To those individuals, creative risk taking is essential to any goal where the stakes are high. Thoughtless risks are destructive, of course, but perhaps even more wasteful is thoughtless caution, which prompts inaction and promotes failure to seize an opportunity.[3]

Aswath Damodaran, a professor at New York University, writes that every major advance that civilizations have made involves someone willing to take a risk by challenging the status quo. He further states that the most successful firms in any industry actively seek out and exploit risk to their own advantage.[4] He states, "Successful firms, over time, can attribute their successes not to avoiding risk but to seeking out and taking the "right" risks. This perspective views risk as an event or activity that may have an impact on an organization's ability to achieve its objectives

or may cause a missed opportunity. The single-minded view that risk is all about avoidance is, in his view, narrow and constraining. It can also be quite paralyzing.

Damodaran's review of risk supports three conclusions that align well with the philosophy of this book. The first is that while some risk definitions focus strictly on the probability of an event occurring, richer perspectives extend this to incorporate a valuation of the consequence of that event. In other words, risk is multidimensional. Throughout this book we will present techniques that consider probability and consequences and model them accordingly. A second conclusion is that in some disciplines a clear distinction is made between a risk and a threat. With this perspective a threat is thought to be a lower probability event while risk is regarded as a higher probability event. Finally, some definitions of risk focus only on the downside of risk, whereas other perspectives are more expansive and consider all variability as risk, including lost opportunities. A company that has more demand for its products than what it is capable of producing appears to have a welcome problem. In reality, the strains placed on that company as it struggles to satisfy demand can affect customer satisfaction, brand reputation, profitability, and even survival.

Each day every company and human being face risk situations. At the individual level, did you drive a car or fly in a plane today? Did you cross a busy street or share the road with cars while riding a bike? Did you eat food at a restaurant where you did not see how the food was prepared? Did you walk down a flight of stairs? Did you step into the shower? Do you have money in the stock market? Did you take an exam without studying? If the answer to even a few of these questions is yes, you have exposed yourself to risk, just like everyone else on the planet. The challenge becomes one of not allowing a fear of risk to paralyze us from pursuing opportunities that are important to our personal and professional advancement. Risk is something we need to manage.

Defining Enterprise Risk Management

It is important to differentiate between enterprise risk management (ERM) and supply chain risk management (SCRM), distinctions that are central to this book. Almost all corporate executives are aware of ERM, a concept that has been around for decades. Using a definition developed by the Aberdeen Group, ERM is

> the process for effective identification, assessment, and management of all significant risks to an entity. This includes not only the traditional areas of financial and hazard risk, but also larger operational and strategic risks. ERM refers to the people, tools, systems, and structures that are part of a broader framework of Governance, Risk, and Compliance.[5]

Chapter 9 will highlight several ERM frameworks, including the then COSO (Committee of Sponsoring Organization of the Treadway Commission) framework and the ISO (International Organization for Standardization) standards relating to risk as well as Governance, Risk, and Compliance.

Corporate executives have been concerned with enterprise risk for years, particularly at publicly traded companies. The Securities and Exchange Commission (SEC) requires publicly traded companies to identify the material risks they face at the corporate level in Section 1A of their company's 10-K report. Failure to identify these risks can result in claims by shareholders that the company did not adequately warn them of potential risks, which could present some liability to a company.

Risk identification within the 10-K reporting requirements is an important part of the ERM process. Historically, the vast majority of risks identified in the 10-K report related to financial and legal risks. Operating and other supply chain risks simply were not perceived as important enough to be addressed at the ERM or 10-K level. Unfortunately, the world has changed and, from a risk perspective, not for the better.

Table 1.1 identifies the enterprise risks identified in Apple's 10-K report. More than one third of the key risks identified by Apple have supply chain connections or implications (those risks are designated with a check mark); something that is becoming increasingly prevalent as supply chain risks earn the dubious "honor" of making the enterprise risk list. While supply chain managers have been asking for increased attention at the corporate level for years, increasing the number of supply chain–related risks on the 10-K report is probably not what they had in mind. Watch what you wish for.

ERM is traditionally the responsibility of finance, treasury, insurance, and legal groups at the corporate level. In fact, a survey by Accenture revealed that at the corporate level, 98% of organizations have what they consider to be a chief risk officer. And, according to Accenture, 96% of risk management owners report to the CEO.[6] With that said, the chief risk officer is often a dual position. At General Motors, for example, the chief risk

TABLE 1. 1

Apple Enterprise Risk Factors: 10-K Report

- Global economic conditions could materially adversely affect the company.
- Global markets for the company's products and services are highly competitive and subject to rapid technological change, and the company may be unable to compete effectively in these markets.
- ✓ To remain competitive and stimulate customer demand, the company must successfully manage frequent product introductions and transitions.
- ✓ The company faces substantial inventory and other asset risk in addition to purchase commitment cancellation risk.
- ✓ Future operating results depend upon the company's ability to obtain components in sufficient quantities.
- ✓ The company depends on component and product manufacturing and logistical services provided by outsourcing partners, many of whom are located outside of the United States.
- ✓ The company relies on third-party intellectual property and digital content, which may not be available to the company on commercially reasonable terms or at all.
- The company is frequently involved in intellectual property litigation and could be found to have infringed on intellectual property rights.
- The company's future performance depends in part on support from third-party software developers.
- ✓ The company depends on the performance of distributors, carriers, and other resellers.
- ✓ The company's retail segment has required and will continue to require a substantial investment and commitment of resources and is subject to numerous risks and uncertainties.
- Investment in new business strategies and acquisitions could disrupt the company's ongoing business and present risks not originally contemplated.
- ✓ The company's products and services may experience quality problems from time to time that can result in decreased sales and operating margin.
- The company is subject to laws and regulations worldwide, changes to which could increase the company's costs and individually or in the aggregate adversely affect the company's business.
- The company's success depends largely on the continued service and availability of key personnel.
- ✓ The company's business may be impacted by political events, war, terrorism, public health issues, natural disasters, and other circumstances.
- The company's business and reputation may be impacted by information technology system failures or network disruptions.
- The company may be subject to breaches of its information technology systems, which could damage business partner and customer relationships, curtail or otherwise adversely impact access to online stores and services, and could subject the company to significant reputational, financial, legal, and operational consequences.

continued

TABLE 1. 1 (continued)

Apple Enterprise Risk Factors: 10-K Report

- The company's business is subject to a variety of U.S. and international laws, rules, policies, and other obligations regarding data protection.
- The company expects its quarterly revenue and operating results to fluctuate.
- The company's stock price is subject to volatility.
- ✓ The company's business is subject to the risks of international operations.
- The company is exposed to credit risk and fluctuations in the market values of its investment portfolio.
- ✓ The company is exposed to credit risk on its trade accounts receivable, vendor nontrade receivables, and prepayments related to long-term supply agreements, and this risk is heightened during periods when economic conditions worsen.
- The company could be impacted by unfavorable results of legal proceedings.
- The company could be subject to changes in its tax rates, the adoption of new U.S. or international tax legislation, or exposure to additional tax liabilities.

officer is also the company's general auditor. At other companies the chief risk officer may be the chief financial officer (CFO). And at some companies the chief risk officer may be part of the insurance group.

Defining Supply Chain Risk Management

Now that we have a working knowledge of ERM, what is supply chain risk management (SCRM)? The definition partly reflects someone's professional discipline or where they reside in the supply chain. In the information technology space, the National Institute for Standards and Technology defines supply chain risk management as a "multidisciplinary practice with a number of interconnected enterprise processes that, when performed correctly, will help departments and agencies manage the risk of using information technology products and services."[7] MITRE, a private, not-for-profit corporation that provides engineering and technical services to the federal government, defines SCRM as "a discipline that addresses the threats and vulnerabilities of commercially acquired information and communications technologies within and used by government information and weapon systems. Through SCRM, systems engineers can minimize the risk to systems and their components obtained from sources that are not trusted or identifiable as well as those that provide inferior material or parts."[8] A third perspective, and the one that most closely aligns with our philosophy, says that supply chain risk management (SCRM) is "the implementation of strategies to manage everyday and exceptional

risks along the supply chain through continuous risk assessment with the objective of reducing vulnerability and ensuring continuity."[9]

One way to view supply chain risk management is to think of it as the intersection of supply chain management and risk management. One thing we know about SCRM is that no standard definition exists. This is one indicator that SCRM is still an evolving discipline. Risk is embedded within so many business disciplines that it should come as no surprise that different groups perceive this concept differently.

WHY FOCUS ON SUPPLY CHAIN RISK MANAGEMENT?

Anecdotal accounts of why supply chain risk management must become a corporate concern are not hard to come by. In fact, we will present dozens of examples that reveal the downside of risk. While natural disasters like hurricanes and floods grab the headlines, the reality is that supply chains face a whole range of risks that most observers believe only to be increasing. A survey by American Productivity and Quality Center (APQC) revealed that 75% of responding companies indicated they were hit by a major supply chain disruption during the two-year period prior to the date of the survey.

A classic example of supply chain risk involves a fire that destroyed an electronics supplier in New Mexico that supplied Nokia and Ericsson with critical components for their phone businesses. The response to this risk event shows the strategic implications of effective (or ineffective) risk management. Nokia's ability to quickly secure components from other sources, compared with Ericsson's lack of preparation for responding to this event, resulted in a dramatic industry shift. Ericsson's supply disruption not only cost the company several hundred million dollars in lost sales, but it essentially ended the company's position as a player in the growing wireless phone business. Chapter 9 will investigate this example in greater detail. Consider some other supply chain risk events:

- A U.S. producer of power tools was surprised to find that the Asian supplier it contracted with to produce its lower-end products began selling those products under its own label in Asia. The U.S. company was further surprised to find that the supplier shared its product designs with other Asian companies. The U.S. producer eventually found itself competing in North America with its own products.

- Some German thieves developed a creative way to steal freight on highways. The thieves position a car in front of a truck to slow it down while another car is positioned next to the truck to prevent it from passing the car in front. Then, a third vehicle pulls up behind the truck and at that point one of the gang members opens the back of the truck to remove cargo. Thieves have used this method to steal cargo more than 50 times.[10]
- Nylon-12 is a critical resin for producing fuel lines and other automotive components. Unfortunately, the resin supply for the entire world is essentially produced in a single facility in Germany. What is even more unfortunate is the explosion that ripped through that plant, taking out half of the world's output in the blink of an eye. Within hours automotive original equipment manufacturers (OEMs) had established crisis management teams to scour the globe for new supply sources.
- Eight heavily armed thieves dressed as police and driving two police vans with flashing lights drove through a hole in the perimeter fence of the Brussels, Belgium, airport and onto a runway. In less than five minutes the thieves opened a plane's cargo door and unloaded 120 packages holding $50 million worth of polished and uncut diamonds. The thieves escaped with the diamonds and are forever embedded in criminal folklore.

We could go on, but you get the idea. Moving beyond anecdotal accounts, an emphasis on supply chain risk management is necessary today because supply chains face many factors that result in higher risk, more so than at any time in modern history. Some of these risk factors are self-inflicted; others are not. IBM researchers have identified a solid set of factors that lead us to a clear conclusion—supply chains are becoming more, rather than less, risky. Table 1.2 summarizes this important set of factors.

Other factors inadvertently expose a company to heightened supply chain risk through unintended consequences. This includes just-in-time delivery and lean systems that result in little to no buffer inventory; a trend toward centralized decision making that may reduce response times and flexibility at local levels; continuous cost reductions that may affect a company's ability to plan and respond to risk events; greater use of single sourcing, which often leaves a company with few supply options and higher supplier switching costs; and widespread outsourcing, potentially leading to a loss of supply chain control. Sometimes we are our own worst enemy.

TABLE 1. 2

Factors That Make Supply Chains Riskier

- Increased globalization through outsourcing, which stretches end-to-end supply chains
- Additional regulatory compliance imposed by government entities, further complicating international trade (such as C-TPAT and SEC conflict mineral reporting requirements)
- Increased levels of economic uncertainty and market volatility, which create additional variability in demand and supply and make it more difficult to accomplish demand–supply planning
- Shorter product life cycles and rapid rates of technology change, which increase the risk of inventory obsolescence
- Demanding customers that create additional time-to-market pressures by requiring better on-time delivery, higher order fill rates, and improved service level efficiencies
- Supply side capacity constraints, making it more difficult to meet demand requirements
- Natural disasters and external environmental events, which affect global supply chains
- Complex networks of suppliers and third-party service providers, as well as large interdependencies among multiple firms, which increase the need to coordinate risk

A study by the Aberdeen Group identified some good reasons why a company should make SCRM an embedded part of its corporate culture. First, a need to protect an organization's brand and competitive advantage is a strategic necessity. Risk events have a nasty way of affecting brand value quickly. Simply think about how stories, whether they are true or not, can impact the value of a brand. Next, the increasing volatility of the global economic environment and markets is resulting in greater risk exposure. Third, corporate mandates to institute and/or improve risk management and governance programs are only going to increase. And, a growing need to comply with new or changing regulatory requirements is forcing a greater emphasis on risk management. Finally, constant pressure to improve shareholder and customer confidence while trying to reduce costs may result in actions that result in greater risk exposure, such as searching for suppliers in untested emerging supply markets.

A range of surveys and studies conclude that supply chain risk is growing. To disregard what has become obvious is short-sighted and dangerous. We can easily cite source after source that concludes essentially the same thing—supply chain risk and its impact on corporate performance continues to grow. It would be challenging to argue that supply chains are, on average, becoming less risky.

Some SCRM Observations

Extensive experience and research enables us to make some observations about the state of risk management. (Chapter 2 will provide a more in-depth presentation of the "as is" state). Perhaps most importantly, most observers have concluded that the potential impact of risk has increased over the last 15 or 20 years. In one survey, almost 75% of risk managers say that supply chain risk levels are higher than in 2005. More than 70% say the financial impact of supply chain disruptions has also increased.[11] And, there is no question that supply markets have become more volatile. The size of fluctuations in commodity prices has more than tripled since 2005 compared with the period of 1980–2005, based on International Monetary Fund data. If you really think about this hard enough, you might just get depressed.

We can also conclude that too many firms are not prepared to handle the supply chain risks that may come their way, even though most managers understand that supply chain risk is a growing concern. While ERM has been at the forefront for many companies, SCRM has been more of an afterthought. A recent study revealed that for firms with less than $500 million in annual revenue (which is the vast majority of companies), only 25% take a proactive approach to risk management.[12]

Another observation is that while many risk categorizations and topologies exist, a convergence appears to be happening around the key categories of supply chain risk—a convergence this book uses. Finally, as it relates to mitigating or lessening the impact of risk events, we tend to see the same set of standard approaches that fail to reflect bold or innovative thinking. While "blocking and tackling" will always be important, it is time to see a bit more creativity and sophistication within the SCRM arena. Later chapters will look at some more advanced SCRM approaches.

Why Aren't We Prepared for SCRM?

The reasons why so many firms are not prepared to manage supply chain risk effectively are varied. We cannot ignore what is perhaps the most likely reason of all—risk management has simply not been a part of the supply chain domain. Why would we focus on something that is not considered all that relevant? It is easy to view the efforts put forth toward risk planning as a big exercise in busy work. This may not be the kind of work that gains personal recognition and promotions.

A study by the Supply Chain Council (SCC) identified a set of barriers that affect the practice of supply chain risk management. One barrier is the tendency of senior management to focus on risk management only during times of crisis, something that needs to shift from responsiveness to prevention. A second barrier is that SCRM requires many functions to cooperate, something that is challenging even on a good day. Third, the study concluded that SCRM responsibilities are typically added to existing staff responsibilities. While everyone should be a risk management stakeholder, adding responsibilities to existing duties clearly creates a competition for resources, a competition that SCRM will often lose. Next, the increasing complexity of products, divisions, regions, and supply chains makes a coordinated SCRM effort more of a challenge. A final barrier is that a partial effort to SCRM dilutes the perceived need for a real and sustained risk management effort. A "close enough is good enough" attitude toward SCRM often prevails. These barriers will clearly affect the state of SCRM.

SOME IMPORTANT RISK CONCEPTS

A working knowledge of some important risk concepts is essential when talking about SCRM, particularly since these concepts are mentioned repeatedly throughout this book. We also do not want someone to appear ill-informed when talking about risk management with others. Part of understanding risk management is having a working knowledge of the terms and concepts that populate this body of knowledge. The following presents some important terms and concepts that will help you speak the language of a risk manager.

Risk Event

An important distinction exists between *risk* and *risk events*. Every day we face hundreds of risks with various probabilities attached to them (although we rarely quantify those probabilities). But, and this is important, a risk is relatively harmless until it happens. There is always a risk that someone will fall off a roof when they are working on their house. Until that person actually takes the plunge, the risk of falling remains simply a risk. If the person falls, the risk is now a *risk event*. A risk event is simple

to conceptualize—it is a risk that has become a reality. Formally defined, a risk event is a discrete, specific occurrence that negatively affects a decision, plan, firm, or organism.[13]

Risk events are not only episodic, temporary occurrences. Risk events can be continuous, particularly if they relate to operational performance problems. Any supply chain performance problem that is ongoing presents continuous risk to multiple parties in a supply chain.

A word of caution is in order here. A tendency exists to identify a grab bag of risk events and then label each event as a risk category. This is generally an unorganized way to approach risk management. Late supplier deliveries or supplier quality problems might comprise two such categories even though they are risk events. Risk events should be organized and placed into broader risk categories. In the supply chain space a number of risks might relate to financial risks, for example, and therefore should be placed under a financial risk category. Subcategories of financial risk may then be developed that include supplier financial risk, working capital risk, or currency risk. A later section will present risk typologies.

Risk Exposure and Vulnerability

Risk exposure involves the quantified potential for loss that might occur as a result of a risk event. The risk exposure value is often the outcome of a comprehensive risk analysis that uses algorithms to combine risks according to their probability of occurring against the potential loss if the risk occurs. A company that can seamlessly switch production between multiple supplier locations has less risk exposure to a supply disruption compared with a buyer that has access to only a single production location. Even before a garment factory collapsed in Bangladesh, killing 430 workers in the country's worst apparel-industry accident, major buyers such as Walmart and Levi Strauss had ceased doing work with vendors who operated in multistory buildings. The risk exposure from these operations was simply too great.[14]

For our purposes we view risk exposure and vulnerability as closely related concepts, although vulnerability tends to be a less quantified concept. We are vulnerable to something if we are susceptible to harm or injury. Anyone who has built a house on an earthquake fault will grasp the concept of vulnerability to earthquakes. Or, someone traveling to certain parts of the world without getting proper vaccinations should appreciate