Preface

Purpose of the Text

Crisis management is a challenge any organization can face and one that many fail. When crisis management fails, stakeholders, and organizations suffer. All organizations must become ready for crises. Boeing, American Airlines, and Deutsche Bank are prominent companies, and each has recently faced crises and handled them with varying degrees of success. Crisis communication is the lifeblood of crisis management because crisis communication brings crisis management to life. When crisis communication is ineffective, so is the crisis management effort. Research about crisis management and crisis communication continues to be produced rapidly in academia and in practice. The vast writings about crisis communication and management remain a blessing and a curse. It is great to have so much information, but it is hard to find and organize it all. The writings about crisis communication and management are fragmented, as people write about crises from very different perspectives. This situation can leave managers struggling to organize bits of information or missing critical resources entirely. Writers often focus on their specialties and fail to make connections to ideas and concepts developed in other specialties (Bundy et al., 2017). In turn, this fragmentation precludes a fuller understanding of crisis communication and management that is gained by integrating the various perspectives. Practitioners, researchers, and educators are limited by this fractured approach.

The primary purpose of this book is to provide a resource that integrates and organizes a wide array of practitioner and academic writings about crisis management. Taken together, this information helps to create evidence-based crisis communication. Evidence-based is an approach taken in any discipline that involves interventions, such as medicine, social work, and management. Crisis communication is an intervention designed to lessen the negative effects of a crisis for stakeholders and the organization in crisis. An evidence-based approach combines the best research with practitioner experience to guide interventions. Practitioners consider the research results and decide if and how they fit their experiences.

The emphasis throughout the book is on the role of communication in the crisis management process. Any discussion of crisis management must include risk and resilience as well. You cannot meaningfully talk about a crisis without including risk. Risk is important throughout the entire crisis management process. Resilience is embedded within crisis management. The point of crisis management has always been to allow those affected by the crisis, stakeholders, and the organization in crisis, to rebound from the disruption a crisis creates. Management in general must recognize the value of strategic crisis communication and the value of crisis management. The book is designed to be a body of knowledge that aids managers, researchers, and educators. *Process* is an important word here. Too many people think that crisis management means having a crisis management plan or responding when a crisis hits. This is a very reactive and rather limited approach to crisis management. A richer, more proactive approach to crisis management explores the entire process.

Audience for the Text

The book is written for both students and practitioners. Students, primarily undergraduates, are given an applied approach to crisis communication that is rooted in theory. Ideally, theory should inform practice, and I have selected the best of the crisis communication and management research for gaining insight into the process. Practitioners can use the book to enhance their understanding and execution of crisis communication. This book is designed to be used to help those who are or may become crisis managers. Any individual with a background in corporate communication, organizational communication, public relations, or management may find themselves on a crisis team. The information in this book should help to make a person a more effective crisis team member. This edition seeks to demonstrate the way artificial intelligence (AI) applications can aid crisis managers at various points in the crisis process.

Organization of the Text

The crisis management process can be organized around three stages: precrisis, crisis event, and postcrisis. The book follows this three-part structure. Chapter 1 provides a discussion of the three-stage approach to crisis management. Chapter 2 highlights the increased importance of social media to crisis management. Chapters 3 and 4 focus on the prevention aspect of precrisis, while Chapters 5 and 6 develop the preparation aspect of precrisis. Chapter 7 concentrates on the crisis event stage, and Chapter 8 explains the postcrisis stage. The epilogue reflects upon key themes within the book.

Pedagogical Features

Throughout the book are "**What Would You Do?**" cases. Each case fits the key points found in a particular chapter. Information from a real crisis event is presented along with a series of questions designed to allow readers to apply text concepts to the case.

This edition retains the **"Crisis Leadership Competencies"** boxes. These boxes highlight the essential leadership skills needed to manage crisis communication effectively in a wide range of situations.

Each chapter ends with a **Chapter Summary** that sums up the main points of the chapter as well as **Discussion Questions** that help readers extend their understanding of the material.

New to the Seventh Edition

Writing a seventh edition of this book was necessary because crisis communication and management is such a dynamic field that it can change significantly in just a few years. Researchers continue to yield additional insights into the crisis management process. Technological innovations and development continue to be a challenge for crisis communication. Examples include how social media platforms and various AI applications have become integrated into crisis management and communication. Researchers have expanded our understanding of crisis communication by developing new ideas, particularly concerning internal crisis communication. We also learn from the professionals on the frontlines wrestling with new developments such as AI applications. The seventh edition tries to capture the more complex view of crisis communication that has emerged from research and practice by translating that material into accessible and usable information for practitioners.

The main changes to the seventh edition are outlined here:

- **Chapter 1** develops the idea of crises as disruptions, especially to the stakeholder–organization relationships and to strategy. An AI primer is included to explain the various AI applications that can be useful to crisis management and communication. The new READINESS model developed by the Crisis Communication Think Tank at the University of Georgia is introduced.

- **Chapter 2** provides an expanded discussion of risk and how it is foundational to crisis management. This expansion includes discussions of the known-unknown framework for risk, more information on the risk matrix, and the value of risk curiosity.

- **Chapter 3** continues the discussion of risk with a presentation of a risk vocabulary and an overview to important ideas from risk communication.

- **Chapter 4** explores the value of training for creating an organization and crisis management team that is ready for a crisis. Decision-making is central to crisis management. Crisis managers must appreciate how this is dynamic decision-making. Also, crisis management teams are subject to stress during crises, and the chapter notes the value in training the team to cope with stress. Organized chaos is introduced as a useful way to think about crisis management.

- **Chapter 5** explores the crisis management plan and adds the escalation protocol to its discussion. The discussion of message mapping is expanded along with the value of assessing the vitality of the organization's crisis communication system and a caution about becoming too dependent on technology when managing a crisis.

- **Chapter 6** explores what the normalcy bias is and how it can create problems for crisis management.

- **Chapter 7** has an expanded discussion of internal crisis communication, considering how employees might become advocates or adversaries during a crisis. How to develop warning messages has been added along with more of a focus on helping crisis victims to cope with the crisis.
- **Chapter 8** adds a discussion of post-alert messaging and how crisis communication can facilitate well-being and healing for crisis victims. It also considers how crisis management can help develop antifragility, thereby moving beyond resilience. The Epilogue section reflects upon the themes of an evidence-based approach to crisis communication, how crisis communication and knowledge management are essential to crisis management, the value of appreciating the internal dimension of crisis management, how crisis management is a form of wayfinding that helps managers navigate the disruptions crises create, and the need to recognize the importance of emotions and well-being in crisis management.

Chapter 1

A Need for More Crisis Management Knowledge

Chapter Objectives

- Define what a crisis is, and differentiate between the various crises.
- Compare and contrast the three-phase mode of crisis management to the regenerative model of crisis management.
- Explain both the external and internal factors that make crisis management important to an organization.

You might have read text or heard podcasts where people say we live in a VUCA world. VUCA stands for volatility, uncertainty, complexity, and ambiguity. A VUCA environment is challenging and rapidly changing. Business experts argue organizations are operating in a VUCA world meaning their environments are dynamic and unpredictable (Arkenberg, 2019). For crisis managers, VUCA has relevance through risks. Risks and crises are inseparable. A risk is the potential to do harm (similar to the sense of the term *threat*), whereas a crisis is the realization of risk. Between the two are issues that indicate the emergence of a risk. Imagine you are hiking in the forest. You see signs warning you that bears are in the area, meaning encountering a bear is a risk. As you are hiking, you see a bear in the distance; the bear is now an issue. Farther along in your hike, a bear charges at you; the bear is now a crisis.

The risk environment organizations face is increasing in complexity and ambiguity. Technology is an important contributing factor to a VUCA risk environment (Arkenberg, 2019). Digitization and artificial intelligence (AI) are two related examples of technology complicating risks. Digitization is the utilization of various digital technologies to enhance task performance. AI, though not new, is the latest technology contributing to digitization (Sanders et al., 2019). AI is actually many things, meaning there are various types of AI. Box 1.1 elaborates on seven highly relevant types of AI for crisis management and communication that will be mentioned throughout this edition. Consider how generative AI is reshaping how many people accomplish tasks (Feuerriegel et al., 2024). Generative AI creates unique text, video, images, and audio. Although generative AI helps people perform tasks, it also increases risks, such as contributing to misinformation (Chu-Ke & Dong, 2024).

Box 1.1 An AI Primer

Artificial intelligence (AI) has been around for decades. AI involves computers simulating human intelligence in some way. AI includes performing human tasks and the AI learns from large data sets. For instance, AI can be trained to identify bone fractures from images such as x-rays. Patterns are the key for AI. AI learns from, identifies, and uses patterns. Large language models (LLMs) are the key to AI. LLMs are a type of deep learning model training using massive data sets. LLMs learn patterns in text allowing them to predict the next word in a text as well as understand nuance and context. LLMs allow humans to manage unstructured data (human language) even at a large scale. LLMs can conduct sentiment analysis, text summarization, and text generation (Stryker, n.d.). LLMs provide the foundation for the various AI applications that are being integrated into crisis management and crisis communication.

For crisis communication and management, seven AI applications are relevant: classification, anomaly detections, predictive, prescriptive, expert systems, generative, and agentic. *Classification* is when AI looks through data, identifies specific patterns based upon the algorithms used to train it, and identifies items. The identification of bone fractures in x-rays is an example of classification AI. In crisis management, classification AI can be used to identify specific risks or types of crises. *Anomaly detection* is a form of classification as well. However, instead of placing items into predefined categories, anomaly detection looks for outliners or aberration in data. Those with a background in statistics will be familiar with outliers or data that do not fit with the rest of the data, what we can call anomalies. AI can identify data that are unusual or deviate from expected values or behaviors (Oracle, n.d.). In crisis management, anomaly detection AI can help to identify signs of failing equipment or safety problems such as visually identifying that a product might have defects prior to shipping.

Predictive AI utilizes historical data to predict future outcomes or trends. In crisis communication, predictive AI can be used to identify how people are likely to respond to specific crisis response strategies. Those predictions are based upon a data set that includes the use of past crisis response strategies and how people reacted to them. It also can be used to anticipate emotional reactions to crises. *Prescriptive* AI goes one step further by recommending specific courses of action to achieve goals. *Expert systems* AI has a logical connection to predictive AI. Predictive AI indicates what might happen while expert systems AI suggests what to do about it. Expert systems AI mimics how experts would analyze a situation and provide guidance based upon that assessment. The AI simulates the decision-making process and abilities of human experts. The expert systems AI seeks "to preserve and replicate human expertise" ("Expert," 2025, para. 2). Expert systems AI is rule-based drawing upon the knowledge base of expert facts and rules to reason through a problem and provide advice on how to solve the problem. In crisis management and communication, the knowledge of experts can be used to create expert AI systems. You can find a variety of such crisis-related expert systems AI online. One example is the Computer-Aided Management of Emergency Operations (CAMEO) developed by the U.S. government. CAMEO "ensures that emergency response personnel have accurate hazardous substance information and assists emergency planners with chemical and all-hazards planning. The software suite is used to access, store, and evaluate information critical for developing emergency plans and responding to emergencies" (Environmental Protection Agency, 2025, para. 2). CAMEO is rule-based using expert knowledge to advise on the creation of protective action recommendations, create maps of expected contamination areas, and provide guidance for emergency managers and first responders.

Generative AI creates unique text, images, audio, and videos based upon prompts it is given by users. It is the most complex of the seven types of AI. ChatGPT made generative AI famous in November 2022. Generative AI draws upon massive amounts of data to find patterns it can use to help it create the content user's request via prompts. In crisis communication, generative AI can help crisis managers write crisis responses that demonstrate empathy. One example is when crisis expert Phillippe Borremans used his emergency alert playbook to guide AI for drafting alerts for crises. His work was used to guide generative AI that can be used to craft crisis alerts (Borremans, 2025b). You also could use generative AI to create a crisis response that sounds like a pirate but that has less utility.

A specialized function within generative AI is summarization, what is called generative AI summarization. A large amount of data, including texts such as meeting notes or social media posts, can be condensed into concise and meaningful summaries. Summarization can be extractive or abstract. Extractive summarization pulls sentences out of the large data set of text to create the summaries; it acts as a highlighter. Abstract summarization writes original sentences to create the summaries; it acts as a writer with a pen. While people find abstract summarization more coherent, there is a greater risk of AI hallucinations (the creation of wrong or misleading information). Extractive summaries are considered more relevant and informative (Murel & Kavlakoglu, 2025).

AI agent and agentic AI are related but different applications used to accomplish tasks. Both utilize other AI applications, including generative AI and predictive AI. AI agent is a tool designed to perform specific tasks and decisions by monitoring its environment, processing information, and acting on specified tasks. Agentic AI can be used to monitor accident reports in an organization to identify patterns and the potential for a crisis to emerge. Agentic AI is system that can coordinate the activities of various AI applications, including multiple AI agents, with high autonomy, reasoning skills, and goal-directed behaviors. An AI agent is a narrow tool while agentic AI is a broad system for orchestrating operations (Outsystems, n.d.; Sapkota et al., 2026). Staying with the risk example, agentic AI could oversee a number of AI agents collecting various risk information, creating a larger picture of the organization's risk environment and anticipating the crises that are likely to emerge.

Agentic AI are systems with autonomy and decision-making abilities. Agentic AI is more advanced than AI agents that are rule based, such as chatbots. Agentic AI will gather and process data (perceive), make informed decisions based on the data (reason), execute tasks derived from the decision (act), and improve performance through feedback loops (learn). And it can do all of this without human intervention. An agentic AI's autonomy can range from supervised to fully independent (Agentic AI, n.d.). Agentic AI can be used in crisis communication to flag specific emerging threats, automate warning systems, facilitate the coordination of multiagency responses, and answer stakeholder inquiries about the crisis.

Any AI is only as good as the data and algorithms used to train it. Before using any specific AI application, review the information about its accuracy (classification, anomaly detection, and predictive AI) and limitations (generative, agentic, and expert systems AI). For instance, generative AI can hallucinate by making up information for you, and using questionable data for predictive AI leads to questionable projections. This edition of the book considers how the various AI applications are being used and can be used in crisis communication and management along with the problems AI presents for crisis managers.

More complex and ambiguous risks help facilitate the manifestation of more complex and ambiguous issues and crises. Researchers and practitioners have documented the increasing complexity of crises (Coombs & Tachkova, 2022; Ramsden-Knowles, 2022; Reber et al., 2021; Tachkova & Coombs, 2022; Whiting & Park, 2023). Researchers from the Crisis Communication Think Tank at the University of Georgia created the label "sticky crises" to capture the crises emerging from these complex and ambiguous risks. "Sticky crises demand not only a near-instant response, but they may require crisis communicators to see possibilities, understand the potential breadth and scope of an emerging crisis, and be ready to change strategy and tactics quickly" (Reber et al., 2021, p. 7). More complex risks result in more complex crises. More complex crises mean greater challenges for crisis managers, a point we shall return to at the end of this chapter.

Developing a comprehensive crisis management program (CCMP) that captures the ongoing nature of crisis management is not an easy task. The crisis management process is varied and requires the integration of knowledge from such diverse areas as small-group decision-making, media relations, environmental scanning, risk assessment, crisis communication, crisis plan development, evaluation methods, disaster sociology, and reputation management. A diverse set of crisis management writings must be navigated in order to develop a complete CCMP that covers every stage and substage of the crisis management process. It is a daunting but necessary task to sort through the plethora of crisis management information to identify the evidence necessary to create evidence-based crisis communication. The most effective way to develop a CCMP is to base your choices on practices and policies that have proven to be effective rather than depending on speculation.

The primary goal of this book is to offer an integrative framework that simplifies the task of organizing crisis management knowledge. An ongoing approach based upon a three-stage model of crisis management provides the foundation. The three stages are precrisis, crisis event, and postcrisis, each of which is composed of substages. The stages are used to summarize and to organize various insights into the crisis management process. Myriad ideas from different areas are synthesized into one continuous process. The end product is a guide for developing each stage in the ongoing crisis management process. This book is a living guide because future developments in crisis management can be easily assimilated into the comprehensive framework of the three-stage approach. The three-stage model articulated here provides a variety of suggestions about how to "do" crisis management. This book is designed to aid those interested in practicing, researching, or teaching crisis management and uses what is called an evidence-based approach. The evidence-based movement started in medicine as a response to the underutilization of scientific evidence in medicine. An evidence-based approach involves the conscious application of multiple sources of evidence to organizational decision-making (Barends & Rousseau, 2018). Four sources of information inform organizational decision-making: scientific findings, practitioner experience, organizational information, and stakeholder concerns. An evidence-based approach to crisis communication draws upon the best crisis communication research (scientific findings from academic and industry research), contextual factors that influence crisis communication (organizational information), and stakeholder concerns that are then viewed through the lens of the crisis managers' own experience with past crises. The book integrates the crisis communication research with practitioner observations, the key contextual factors, and salient stakeholder concerns.

To those interested in the practice, the book offers a comprehensive approach for structuring a crisis management program. For crisis managers, the book is more useful to those just starting in the practice. Experienced crisis managers might learn something new but have strongly honed experiences to help guide their crisis decision-making. Newer crisis managers can benefit more from the lessons offered by research and the experiences of other practitioners. For those interested in research, the book provides an analytic framework for the study of crisis management efforts. Those involved in teaching are offered an additional resource for educating future crisis managers. The book ends with a summary of key ideas and highlights some of the insights offered to practitioners, researchers, and educators.

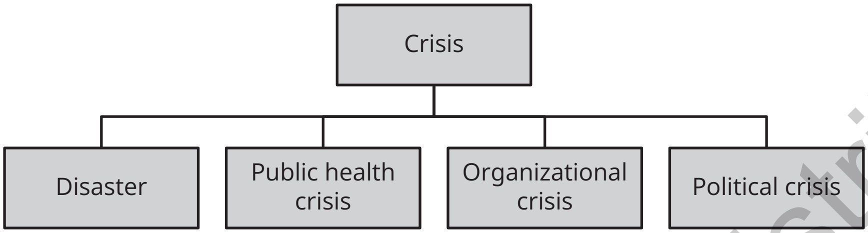
Crisis Management Defined

There are a lot of books written about crisis management, but there is no one accepted definition of a crisis. Having a specific definition is important because how a subject is defined indicates how it is approached.

Crisis is a very broad term that is used frequently by practitioners and academics. It is useful to think of crisis as a disruption. A crisis disrupts relationships, particularly the relationship between the organization in crisis and its constituents. Consider how customers and suppliers need to alter their relationships with a food company when that company has to recall a product due to contamination by a foodborne pathogen. A crisis disrupts the organization's strategy. Managers need to focus attention, time, and resources on the crisis rather than the pursuit of strategic goals. The crisis will impact organizational strategy because the organization will not be exactly the same after a crisis. When Macy's found one employee had hidden over $150 million in delivery costs, a new system for overseeing financial controls had to be created (M. Wilson, 2024). And crises can disrupt operations to varying degrees. Industrial accidents can shut down a facility, product recalls can stop production of products, and the death or abrupt resignation or removal of a CEO can create turmoil with succession. We can rightly define crisis broadly as a disruption.

It is important to specify early in the book what I mean by the term *crisis* and differentiate it from similar concepts. Figure 1.1 is a visual representation of how I conceptualize crisis. We can take the general notion of crisis as the starting point, beneath which we have disaster, public health crisis, organizational crisis, and political crisis.

Figure 1.1 ▪ Types of Crises



Disaster Defined

Disasters are events that are sudden, seriously disrupt routines of systems, require new courses of action to cope with the disruption, and pose a danger to values and social goals (Quarantelli, 2005). This is more a set of characteristics than a definition, but it does capture the nature of disasters. I would add that disasters are large in scale and require response from multiple governmental units. Disasters can spawn organizational crises. For instance, an organization may need to cope with the effects of the disaster on its operation. An example would be utilities needing to restore power to customers following a tornado. In rarer circumstances, a crisis can trigger a disaster. Examples include the Union Carbide toxic gas release in Bhopal, India, and the crude oil spilled into the Gulf of Mexico when the Deepwater Horizon sank. Research has generated a significant amount of advice on how to cope with disasters, and there is some overlap between disasters and organizational crisis efforts. However, this book focuses on organizational crises. I choose to present a very specific definition of organizational crisis to clarify for the readers how this book will approach crises.

Public Health Crisis Defined

Public health crises are a threat to public health that exists across multiple geographic areas (Maibach & Holtgrave, 1995). In addition, a public health crisis has the potential to overwhelm the routine community capacity to manage it (C. Nelson et al., 2007). COVID-19, SARS, and Ebola are examples of public health crises, as are slower moving crises such as vaping. The health component is the unique dimension of public health crises. Human health is affected across a range of areas and can be more than the health care system can manage. Consider how the health care system in New York City was overwhelmed during the early stages of the COVID-19 pandemic. Disasters can spawn a public health crisis by triggering disease outbreaks. Government actors and nongovernmental organizations (NGOs) take the lead in managing public health crises. However, as illustrated by the COVID-19 pandemic, organizations can be affected by public health crises and must prepare for that potentiality.

Organizational Crisis Defined

An organizational crisis is the perceived violation of salient stakeholder expectations that can create negative outcomes for stakeholders and/or the organization. This definition is a synthesis of various perspectives on crisis that tries to capture the common traits other writers have used when describing crises.

A crisis is perceptual. What we typically think of as crises are events that are easy to perceive as such. That is why few people would dispute industrial accidents or hurricanes being crises. However, it is the perceptions of stakeholders that help to define an event as a crisis. A stakeholder is a person or group that is affected by or can affect an organization (Bryson, 2004; Freeman, 1984). If stakeholders believe an organization is in crisis, a crisis does exist, and stakeholders will react to the organization as if it is in crisis. For nearly a decade, the automobile manufacturer Audi told its customers there was nothing wrong with its transmissions. However, customers did perceive a crisis because a few cars were jumping into gear from neutral—with sudden acceleration—resulting in injuries and deaths. We fast-forward to 2009, and Toyota was wrestling with gas pedals that stick, causing cars to accelerate uncontrollably and at times fatally. Toyota was criticized for a slow response to the crisis. Toyota management had a difficult time seeing the problem and realizing the organization was in a crisis. Management must be able to see the event from the stakeholders' perspective to properly assess whether a crisis has occurred.

Crises can violate salient expectations that stakeholders hold about how organizations should act. These expectations are important to the stakeholders and can be related to health, safety, environmental, or economic concerns. Planes should land safely, products should not harm us, management should not steal money, and organizations should reflect societal values. Crises disturb some stakeholder expectations, resulting in people becoming upset and angry, which threatens the relationship between the organization and its stakeholders. That is why crises are considered dangerous to organizational reputations (Barton, 2001; Dilenschneider, 2000). A reputation is how stakeholders perceive the organization. When expectations are breached, stakeholders perceive the organization less positively: The reputation is harmed.

Crises have the potential to create negative or undesirable outcomes for stakeholders and organizations. Product harms crises place customers at risk for injury or death. If business is disrupted, an organization will usually suffer financial losses (e.g., lost productivity, a drop in earnings). Crisis damage extends beyond financial loss, however, to include injuries or deaths to stakeholders, structural or property damage (on and off site), tarnishing of a reputation/social evaluations, damage to a brand, and environmental harm (Loewendick, 1993). The damage can affect a variety of stakeholders. A plane crash can kill crew members, passengers, and people on the ground. In addition, an entire industry can be affected by a crisis for just one of its member organizations. An industry can suffer financial loss (e.g., new, costly regulations) or reputational damage as people project a localized crisis onto an entire industry. In 2006, the cruise ship industry became involved in the Carnival Cruise Lines fire because the crisis was an industry-wide threat, not just a company-specific one. Fires were a risk on every cruise ship, and people needed to feel safe. Employees, customers, or community members can be injured or killed by industrial or transportation accidents.

Environmental damage is another outcome of accidents. Community members can suffer structural or property damage from accidents as well. Explosions can shatter windows, and evacuations can cost community members in terms of money, time, and disruption. Careless handling of an accident can add to the damage. Investors can lose money from the costs of the crisis. For example, an organization can incur repair expenses from an accident while a faulty product can result in product liability lawsuits and recall costs. A crisis presents real or potential negative outcomes for stakeholders, the organization, and even the industry. Crisis management is designed to ward off or reduce the threats by providing guidance for properly handling crises. The negative outcomes from crises are what bind it to resilience. Stakeholders and organizations must be able to bounce back from the shocks created by crises.

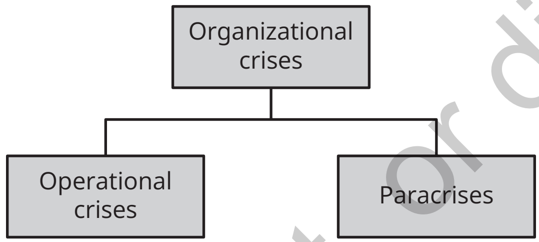
One final point to mention is the unpredictable nature of crises. A crisis is unpredictable but not unexpected. Wise organizations know that crises will befall them; they just do not know when. Crises can be anticipated, but their often sudden nature can give them an element of surprise or unpredictability (Barton, 2001; National Research Council, 1996). However, some crises offer a great deal of warning (Irvine & Millar, 1996). For instance, if a major television news magazine is planning to run a negative story about an organization, management will know about the event months in advance. Metabolife, a diet supplement company, faced just such a crisis in 1999. It used the lead time to create an aggressive multimedia campaign to defend itself from charges linking its product to harmful side effects. Radio and newspaper advertisements were used to drive people to a specially created website where people could watch an unedited video of the interview and learn how news shows can distort the truth.

At this point, it is instructive to further separate organizational crises into operational crisis and paracrises. Operational crises reflect the roots of crisis management itself. One potential effect from a crisis is to disrupt operations either completely or partially. Many early definitions of crisis included disruption of operations as a key component (e.g., Barton, 2001). Crisis management was developed in part to limit disruptions to operations because an organization loses money when it is not operating at full capacity. Business continuity, a sister discipline to crisis management, is dedicated to preventing or limiting operational disruptions. Operational crises capture those situations where there is actual or potential disruption to organizational operations. Facility fires, natural disasters, and product harm situations are all examples of operational crises. I will elaborate on the various types of operational crises in Chapter 4. Operational crises create some specific communicative demands for crisis managers because they must consider the information needs of various stakeholders when there are disruptions. For instance, employees need to know when, if, and where they are working while suppliers and customers need to know if there will be deliveries and shipments and the size of those deliveries and shipments.

Paracrises are situations where crisis managers must manage a crisis risk in full view of its stakeholders (Coombs & Holladay, 2012c). Paracrises reflect the reputational/social evaluation focus of many crises. All crises will inflict some reputational damage on an organization.

However, certain situations are primarily reputational and have limited effects on operations. The terms *reputational crises* and *social media crises* have been used in attempts to capture the emphasis on reputational concerns. The term *reputational crisis* is confusing because reputation also is an antecedent and consequence for a crisis and because all crises have a reputational dimension. The term *social media crisis* is extremely vague, referring to events that transpire in or are intensified by social media. Again, any crisis can have a social media aspect to it, and labeling a crisis by the dominant media involved is imprecise. Instead, I prefer to make a distinction between organizational crises that are operational crises and paracrises, as illustrated in Figure 1.2.

Figure 1.2 ▪ Operational Crises and Paracrises



The prefix *para-* means resembling or protecting from something. A paracrisis resembles a crisis because it threatens the organization's reputation and related assets. However, a paracrisis would not require the activation of the crisis team and does not disrupt the organization. Still, a paracrisis warrants attention because neglect or mismanagement could escalate into an operational crisis. A paracrisis is a specific type of crisis warning sign. It mimics a crisis itself. Motrin's offensive ad to mothers is an example of a paracrisis. In 2008, Motrin created an edgy ad that noted how mothers have back pain from using sling-type baby carriers. The ad was in print and online in video form. Many mothers were offended by it and took to social media to express their outrage. Twitter (now X) was a popular location for mothers to attack Motrin. There was even a nine-minute YouTube video featuring the Twitter complaints. The ad appeared online on a Saturday morning. The social media criticism stormed Twitter by Saturday evening. On the following Monday, McNeil Consumer Healthcare, the maker of Motrin, removed the ad from the Internet and replaced it with an apology (Tsouderos, 2008). McNeil Consumer Healthcare did not see any disruption in the production or sale of Motrin. There was minor damage to the corporate and brand reputation that had the potential to escalate if the paracrisis was not handled swiftly and effectively. By removing the ad and apologizing, McNeil Consumer Healthcare managed the paracrisis, thereby defusing a potential crisis.

Paracrises that emerge in digital communication channels and platforms such as social media are unique crisis warning signs (crisis risks) because they appear in full view of stakeholders. Typically, crisis prevention efforts are invisible to stakeholders. For instance, organizations might revise safety procedures or replace a dangerous chemical to reduce the threat of hazardous chemical releases. Visibility is what gives a paracrisis its impact. Moreover, organizational stakeholders are driving the risk by raising it as a public concern (Coombs & Holladay, 2012c). The public appearance of the paracrisis demands public management. Managers must explain to all stakeholders what is being done to address the concern or why they are choosing to ignore it. The paracrisis blurs the line between precrisis and crisis response because addressing the paracrisis can appear to be a crisis response rather than mitigation actions. The key point here is that the digital communication channels and platforms increase the visibility and number of paracrises because the Internet can highlight the stakeholder concerns that drive paracrises. The feeling about crisis experts is managers should not ignore conflicts or crises emerging on social media (e.g., Bernstein, n.d.). I discuss the various types of paracrises and response options in Chapters 2 and 3 as part of the explanation of the links between risk management and crisis management.

What Would You Do?

Rio Tinto Destruction of a Heritage Site: Act 1

On May 24, 2020, the extraction company Rio Tinto expanded its Brockman 4 iron mine by demolishing parts of the Juukan Gorge in Western Australia's Pilbara region. The explosions destroyed rock shelters considered sacred to the Puutu Kunti Kurrama and Pinikura (PKKP) people. It was a 46,000-year-old Indigenous site. The PKKP people had expressed concern about the shelters to representatives of Rio Tinto. The blast was legal under Section 18 of the Aboriginal Heritage Act of 1972. You are part of Rio Tinto's crisis management team. News has just broken that blasting at Juukan Gorge destroyed a 46,000-year-old Aboriginal site of immense cultural significance. Social media outrage is escalating, investors are starting to contact headquarters, and Indigenous leaders are publicly condemning the company. This is a situation that actually happened. What do you do next? Who are your most important stakeholders and why? What immediate actions might you recommend be taken and why?

Political Crisis Defined

Political crises center on political power, including efforts to boost one's own power or to undercut the opposition's power. On one level, political crises create expectations among citizens, and an effective crisis response must live up to the expectations of the citizens. It is assumed political leaders will protect society from the negative effects of a crisis (Boin et al., 2016). On a second level, political crisis can be exploited for political gains. Exploiting crisis involves framing contests, including efforts to frame the significance of a crisis and the causality of the crisis. Crisis exploitation is the "purposeful utilization of crisis-type rhetoric to significantly alter levels of political support for public office-holders and public policy" (Boin et al., 2009, p. 83). This level reflects the political nature of crises and way crises can create or intensify division (Boin et al., 2016). Any crisis can have a political dimension to it as disasters, corporate crises, and public health crises have been politicized. We will explore some of the politicization of crises in Chapter 2 in the discussion of paracrises and affective polarization.

Crisis Management

Crisis management represents a set of factors designed to combat crises, to lessen the actual damage inflicted, and to facilitate resilience. Put another way, it seeks to prevent or lessen the negative outcomes of a crisis and thereby protect the organization, stakeholders, and industry from harm while facilitating positive response to the situation. Crisis management has evolved from emergency preparedness and, drawing from that base, comprises a set of four interrelated factors: prevention, preparation, response, and revision.

Prevention, also known as mitigation, represents the steps taken to avoid crises. Crisis managers often detect warning signs and then take actions designed to prevent the crisis. For instance, a faulty toaster is recalled before its overheating problem causes any fires or injuries to customers. Prevention is largely unseen by the public. News stories about crises that did not happen are rare.

Preparation is the best-known factor in crisis management because it includes the crisis communication plan (CCP). If people know nothing else about crisis management, they know an organization should have a CCP. The CCP is the tip of the crisis management iceberg. Although people think the CCP is the crisis management process, in actuality, most of the process is unseen. Preparation also involves diagnosing crisis vulnerabilities, selecting and training a crisis management team and spokespersons, creating a crisis portfolio, and refining a crisis communication system. Preparation creates a more agile organization and fosters both individual and organizational resilience.

Response is the application of the preparation components to a crisis. A crisis can be simulated (as in an exercise) or real. The preparation components must be tested regularly. The testing involves running simulated crises and drills that determine the fitness of the CCP, crisis team members, spokespersons, and the communication system. A real crisis involves the execution of the same crisis management resources, only the outcomes are real rather than hypothetical. Response is very public during an actual crisis. An organization's crisis management response is frequently reported and critiqued in the news media (Pearson & Clair, 1998). Many publications critiqued Bausch & Lomb's failure to recall ReNu with MoistureLoc when it was linked to a 2006 outbreak of Fusarium keratitis, a form of fungal eye infection that can produce blindness (Dobbin, 2006; Mintz & Di Meglio, 2006). Bausch & Lomb did stop shipping the product and eventually asked retailers to remove the product from shelves. However, it was not until May 15, a month after the crisis began, that an official recall was issued (Mintz & Di Meglio, 2006). Remember, crises make for good news stories, and news of ReNu with MoistureLoc was everywhere. We witnessed a similar pattern of intense media coverage for Volkswagen's poor handling of its dieselgate crisis (Clemente & Gabbioneta, 2017).

In an actual crisis, responses seek to achieve outcomes related to reducing the negative impact of a crisis on stakeholders and the organization. Put another way, the response helps to achieve the objectives of crisis management. Organizations try to limit the threat to public safety, reputational erosion, brand damage, and loss of sales, to name but a few of the common crisis communication objectives. There is even a chance that the response leads to an improved organization. Improvements can include a stronger reputation, a more powerful brand, and changes to the organization that make it a safer place to work.

Part of the response is *recovery*, which denotes the organization's attempts to return to normal operations as soon as possible following a crisis. Resilience is the key to recovery because the capacity to be resilient facilitates recovery. *Business continuity* is the name used to cover the efforts to restore operations to normal. As noted earlier, downtime from a crisis is a financial drain. The quicker an organization can return to normal operations, the fewer financial losses it will incur.

Revision is the fourth crisis factor. It involves evaluation of the organization's response in simulated and real crises, determining what it did right and what it did wrong during its crisis management performance. The organization uses this insight to revise its prevention, preparation, and response efforts. Ideally, in the future, the right moves are replayed while the mistakes are avoided and replaced by more appropriate actions. Revision is the development of an institutional or organizational memory, which can improve the effectiveness of crisis management by expanding the organization's perception of crises and its response capacity (A. Li et al., 2004; Weick, 1988). The more and varied the crises an organization experiences through practice sessions, the better it can handle similar situations in reality. The factors are linked in a spiral. If prevention fails, preparation is required for optimal performance. Revision is derived from performance and informs both the prevention of and preparation for future crises. In turn, improving preparation should improve response.

Crisis management is brought to life through crisis communication. A crisis management plan is just a document. The crisis teams enact the crisis management plans by talking about the crisis with one another and those outside of the crisis management team. We can broadly define crisis communication as the enactment of crisis management. However, the most visible aspect of crisis communication is the crisis response. Crisis responses are interventions designed to lessen the negative effects of the crisis. (See Chapter 7 for a detailed discussion of the crisis response).

Understanding the crisis management process is a necessity for effective crisis communication. We can extend the notion of process by creating a framework for crisis management that involves distinct stages that influence one another.

The Initial Crisis Management Framework

The idea that crises have an identifiable life cycle is a consistent theme that permeates the crisis management literature. This section explores crisis management as a process. The life cycle approach is explained along with details on the three-stage approach to crisis management and the regenerative model of crisis management. The section concludes by explaining the importance of social evaluations (centering on reputation) to crisis management.

Why a Life Cycle Approach to Crisis Management

The crisis manager needs to understand this life cycle because its different phases require different actions (Gonzalez-Herrero & Pratt, 1995; Sturges, 1994). The crisis life cycle has been translated into what I term *staged approaches* to crisis management. A staged approach means that the crisis management function is divided into discrete segments that are executed in a specific order. Moreover, the life cycle perspective reveals that effective crisis management must be integrated into the normal operations of an organization. Crisis management is not merely developing a plan and executing it during a crisis. Instead, it is appropriately viewed as an ongoing process. Every day, organization members can be scanning for potential crises, taking actions to prevent/mitigate them, or considering any number of the aspects of the crisis management process detailed in this book. Crisis management should be a part of many people's full-time jobs in an organization, not a part-time fancy. Each working day, crisis managers can be doing something to improve crisis prevention and response (Coombs, 2006a).

The life cycle perspective has yielded a variety of staged approaches to crisis management. These provide a mechanism for constructing a framework for organizing the vast and varied crisis management writings and for creating a unified set of crisis management guidelines. Regardless of the discipline, the various topics addressed can be placed within a comprehensive, incremental approach to crisis management. An overarching framework organizes the scattered crisis management insights and permits crisis managers to easily envision their best options during any stage of the process. Crisis managers can find it easier to access and apply available resources, thereby improving the crisis management process. The framework I use in this book is influenced by existing models of the process. Reviewing these models will reinforce the importance of process in crisis management.

Fink's (1986) four-stage model is the earliest staged approach to crisis and can be found in his seminal book, *Crisis Management: Planning for the Inevitable.* His cycle is well represented in writings that have appeared since the 1990s. He uses a medical illness metaphor to identify four stages in the crisis life cycle: (1) prodromal: clues or hints of a potential crisis begin to emerge; (2) crisis breakout or acute: a triggering event occurs along with the attendant damage; (3) chronic: the effects of the crisis linger as efforts to clean up the crisis progress; and (4) resolution: there is some clear signal that the crisis is no longer a concern to stakeholders—it is over.

Fink's (1986) approach is one of the first to treat a crisis as an extended event. Of particular note is his belief that warning signs precede the trigger event. The job of crisis managers expands and becomes more proactive when they know and read the warning signs. Well-prepared crisis managers do not just enact the CCP when a crisis hits (being reactive); they are also involved in identifying and resolving situations that could become or lead to a crisis (being proactive). In addition, Fink divides the crisis event into three stages. A crisis does not just happen; rather, it evolves. It begins with a trigger event (acute phase), moves to extended efforts to deal with the crisis (chronic phase), and concludes with a clear ending (resolution). The different stages of the life cycle require different actions from the crisis manager. As a result, crisis management is enacted in stages and is not one simple action. The demands of the crisis stage dictate what crisis managers can and should be doing at any particular time.

Richardson (1994) provides one of the earliest detailed discussion of the three components: (1) precrisis or predisaster phase: warning signs appear and people try to eliminate the risk; (2) crisis impact or rescue phase: the crisis hits and support is provided for those involved in it; and (3) recovery or demise phase: stakeholder confidence is restored. Others using the three-staged model include Ian Mitroff (1994), Birch (1994), Guth (1995), and T. H. Mitchell (1986). Following from this three-stage approach, I divide the crisis management process into three macrostages: precrisis, crisis, and postcrisis. The term *macro* indicates that the stages are general and that each contains a number of more specific substages: the microlevel. This is similar to economics, where macroeconomics deals with all the forces at work on the economy while microeconomics deals with specific factors.

Outline of the Three-Stage Approach

The ideal crisis management model accommodates the various crisis models plus additional insights provided by other crisis management experts. Not all crisis managers have placed their ideas within a phased model. Therefore, a comprehensive model must be able to place random insights into the crisis management process. The three-stage approach has the appropriate macro-level generality for constructing the comprehensive framework necessary for analyzing the crisis management literature. The three stages are general enough to accommodate the other two dominant crisis management models and to allow for the integration of ideas from other crisis management experts.

Within each stage there are separate substages or sets of actions that should be covered during that stage. Each substage integrates a cluster of writings about that particular crisis management topic. Each cluster of writings has been carefully examined to distill the essential recommendations they could offer to crisis managers. For each substage, the crisis wisdom and any tests of that wisdom are reported, along with a discussion of its utility, to crisis managers. Moreover, this three-stage approach provides a unified system for organizing and utilizing the varied insights crisis managers offer.

Precrisis

The precrisis stage involves three substages: (1) signal detection, (2) prevention, and (3) crisis preparation. Chapters 2, 3, 4, and 5 are devoted to the development of this stage. Organization members should be proactive and take all possible actions to prevent/mitigate crises. The precrisis stage entails actions to be performed before a crisis is encountered. However, not all crises can be prevented, so organization members must prepare for crises as well.

Chapter 2 develops the links between risk and crisis. Chapter 3 deals with signal detection with an emphasis on mitigating crises. Most crises emit early warning signs. If early action is taken, these crises can be avoided (Gonzalez-Herrero & Pratt, 1995). Crisis managers must identify sources for warning signs, collect information related to them, and analyze the information. For example, a pattern in customer complaints could identify a product defect. Reporting the complaints to the appropriate manufacturing sector of the organization could result in corrective action being taken. In turn, the corrective action could prevent further complaints and the potential of a highly visible recall, battle with customers, or both. Crisis managers must develop a system for detecting potential crises and responding to them, what is called risk management. Risk management is actually a form of resilience.

Chapters 4 and 5 develop the idea of crisis preparation. Crisis managers must be prepared for a crisis happening. Preparation typically involves identifying crisis vulnerabilities, creating crisis teams, selecting spokespersons, drafting CCPs, developing crisis portfolios (a list of the most likely crises to befall an organization), and structuring the crisis communication system. Preparation helps to build a capacity for resilience.

Crisis Event

This stage begins with either a trigger event that marks the beginning of the crisis or managers realizing they are in a crisis. The crisis stage ends when the crisis is considered to be resolved. During the crisis event, crisis managers must realize that the organization is in crisis and take appropriate actions. This phase has two substages: (1) crisis recognition and (2) crisis containment. Communication with stakeholders is a critical facet of this phase. An organization communicates to stakeholders through its words and actions.

Chapter 6 is devoted to crisis recognition. People in an organization must realize that a crisis exists and respond to the event as a crisis. Crisis recognition includes an understanding of how events get labeled and accepted as crises—how to sell a crisis to management—and the means for collecting crisis-related information. Chapter 7 covers the crisis response and includes topics related to crisis containment and recovery. Crisis containment focuses on the organization's crisis response, including the importance and content of the initial response, communication's relationship to reputational management, contingency plans, and follow-up concerns. The crisis response allows individuals and organization to demonstrate their resilience.

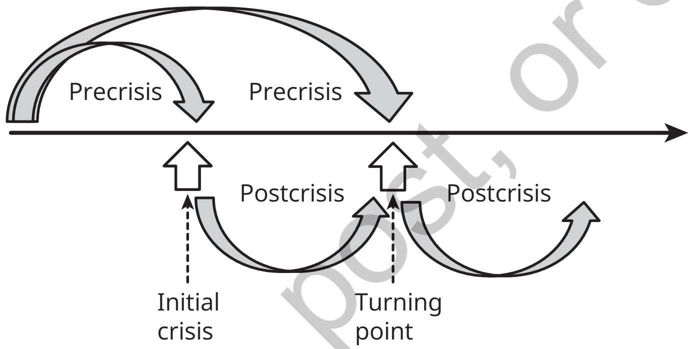
Postcrisis

When a crisis is resolved and deemed to be over, an organization must consider what to do next. Postcrisis actions help to (a) make the organization better prepared for the next crisis, (b) make sure stakeholders are left with a positive impression of the organization's crisis management efforts, and (c) check to make sure that the crisis is truly over. Chapter 8 addresses evaluating crisis management, learning from the crisis, and other postcrisis actions, such as follow-up communication with stakeholders, mourning, and continued monitoring of issues related to the crisis. The ability to recover is a direct reflection of resilience.

A More Advanced View: The Regenerative Model of Crisis

The regenerative model of crisis offers a more complex and dynamic view of a crisis situation. While composed of only two phases, the regenerative model is dynamic because it explains how crises can become reframed and produce significant communicative shifts for crisis managers. The regenerative model is composed of the precrisis and postcrisis phases. The precrisis phase consists of all factors that occur prior to a crisis. The crisis is simply a point in time. The initial crisis is either an event or a realization. An event is some action that demonstrates the existence of a crisis, such as an explosion or people becoming ill from a food product. A realization is when managers recognize that stakeholders view the organization as violating key expectations, such as the quality of the product or service. The turning point is the dynamic aspect of the regenerative model that introduces complexity. A turning point occurs when events or actions reframe and redefine the crisis. Essentially a new crisis emerges because various factors have led people involved with the crisis to view it as a new crisis type. An example is the analysis of Dow Corning Corporation and the breast implant crisis by Brinson and Benoit (1996). Their analysis reveals turning points were evidence, and communicative actions effectively reframed the crisis into a new crisis type. When a turning point occurs, what had been the postcrisis phases, such as actions taken by the organization, now become part of the precrisis phases and a new postcrisis phase begins (Coombs, 2017a). Figure 1.3 illustrates the dynamic nature of the regenerative crisis.

Figure 1.3 ▪ Regenerative Crisis Model



Not all crises are complex enough to fit the regenerative crisis model. Still, crisis managers must be aware that a crisis can suddenly shift from one crisis type to another. Along with this shift will be new communicative demands. Crisis managers might have to change communicative responses to reflect the new demands of an evolving crisis. In fact, the initial crisis response might be the reason stakeholder views of the crisis have shifted, what Frandsen and Johansen (2017) term a *double crisis*. The need to change crisis response strategies is problematic because changing strategies creates the appearance of inconsistency. However, the changes are necessary when a crisis is significantly reframed to a new crisis type.

What Would You Do?

Data Breach at Ashtech Corporation: Act 1

You work at AshTech Corporation, a mid-sized technology services company employing 500 people across two offices. The company handles sensitive client data, including financial records, personal identifiers, and proprietary project information. It is 8:45 a.m. on a Tuesday. A member of the IT security team notices unusual activity on the company's servers involving large data transfers occurring overnight to an unrecognized external IP address. Also, a number of employees have reported being locked out of their company email accounts. The chief information security officer has been notified and has just confirmed there is credible suspicion of a data breach.

What should you do next to help prepare for the crisis now that it is possible sensitive client data have been compromised?

Who are your primary stakeholders and why?

What actions should your organization be taking?

How might you communicate these actions to your stakeholders?

Importance of Crisis Management

The first paragraph of this chapter offers a reminder that crises are ubiquitous. In fact, today's environment seems to be placing higher premiums on crisis management; unprepared organizations have more to lose today than ever before. A variety of developments has made all types of organizations more susceptible to crises. Managers have identified the following as common negative effects from crises: decrease in revenue, cutbacks and/or layoffs, loss of corporate reputation, increased media scrutiny, increased government scrutiny, decreased share price, and increased social media discussions (Burson-Marsteller & Penn Schoen Berland, 2011; Spencer Stuart & Weber Shandwick, 2012). The developments that increase the need for effective crisis management are an increased value of reputation (social evaluations), stakeholder activism, the emergence of digital naturals, broader views of crises, negligent failure to plan, and employer duty of care.

Value of Social Evaluations

Crisis managers do worry about the effects of a crisis on the organizational reputation (Barton, 2001; Burson-Marsteller & Penn Schoen Berland, 2011; Davies et al., 2003; Dilenschneider, 2000). Reputation is part of a broader concept known as social evaluations. Social evaluations are the "socially constructed, collective perceptions of firms" (Pollock et al., 2019, p. 444). Social evaluations are some mix of the three evaluative dimensions of rational, emotional, and moral. Rational uses an analytic approach to assessing an organization's worth and capabilities.

Emotional represents emotional reactions that are more instantaneous but can have long-term consequence. Moral is the degree to which an organization meets or violates commonly held stakeholder or societal values (Pollock et al., 2019). Social approval is a form of social evaluation that is "an overarching construct to describe the more intuitive and affective perceptions inherent in the social evaluation of an organization" (Bundy & Pfarrer, 2015, p. 348). Social approvals reflect how stakeholders feel about an organization.

Social approval assets are favorable collective perceptions stakeholders have for an organization. Social disapproval liabilities arise from unfavorable collective perceptions stakeholders have for an organization (Pfarrer et al., 2010). Overall, social approval represents fast thinking and the intuitive aspect of sense-making (Kahneman & Frederick, 2002). It is more about affective reasoning than rational thought. Though the link between crises and reputation is strong, it is more accurate to think of crises in terms of social approval rather than reputation because social approval captures the immediate reactions to crises. The concern for crisis managers is that a crisis creates a social disapproval liability. Social disapproval liabilities threaten a number of organizational assets, including attracting customers, generating investment interest, attracting top employee talent, motivating workers, increasing job satisfaction, generating more positive media coverage, and garnering positive comments from financial analysts (Alsop, 2004; Davies et al., 2003; Dowling, 2002; Fombrun & van Riel, 2004; Y. Kim & Yang, 2013; van Riel, 2013). As greater emphasis is placed on reputation and other social approvals, a corresponding emphasis must be placed on crisis management as a means of protecting against social disapproval liabilities (Coombs & Holladay, 2002; Pfarrer et al., 2010).

Stakeholder Activism

Today, angry stakeholders are more likely to generate crises than in the past (Lye & Muller, 2004). Consumers, shareholders, employees, community groups, and activists are becoming increasingly vocal when dealing with organizations and are using the Internet to voice those concerns (Coombs, 2002; Heath, 1998). Consider how the Internet was leveraged to advocate for social justice during the spring of 2020 and Black Lives Matter (BLM). The Internet provides various means of stakeholder expression, including web pages, discussion boards, blogs, microblogs, social networks, and content-sharing sites. The key feature of these Internet channels and platforms is the ability of users to create the content rather than just the organizations. Collectively, the Internet platforms where stakeholders create the content are called *social media*. The vast majority of social media messages never find an audience. However, when disgruntled stakeholders strike a responsive chord and connect with other stakeholders online, a crisis can occur. These crises evolve from the value of the organizational reputation. Legitimate criticism that spreads among stakeholders poses a direct threat to the organization's reputation. Here's an example: In 2025, the U.S. restaurant chain Cracker Barrel released a revamped logo as part of its ongoing effort to revitalize the brand. Other revitalization efforts included menu changes and some décor alterations. Stakeholders reacted negatively to the logo change, including attacks of the company on social media platforms and blistering comments in the traditional media. It is natural for customers to dislike corporate logo changes because of consumer nostalgia for the old logo. The customers have positive feelings for the old logo as they are nostalgic for the past (Shields & Johnson, 2016). However, the Cracker Barrel backlash was supercharged through the divisive diversity, equity, and inclusion (DEI) discussion in the United States. Conservatives claimed the logo chain was a sign Cracker Barrel was "woke" and embracing DEI (Graham, 2025). Within 10 days, Cracker Barrel dropped the old logo by saying, "We thank our guests for sharing your voices and love for Cracker Barrel. We said we would listen, and we have. Our new logo is going away" (Cracker Barrel, 2025, para. 1). The restaurant chain experienced a dip in sales during the 10 days of the new logo (Graham, 2025). This demonstrates the ability of stakeholders to leverage social and traditional media to pressure an organization into changing its behavior.

Activist groups are using the Internet to organize and to pressure organizations to change their behaviors. Social media is part of a mix of pressure tactics, along with negative publicity campaigns and boycotts. For instance, the Enough Project utilized Facebook, Twitter (now X), YouTube, Flickr, and Instagram in its efforts to pressure electronics companies into disclosing their sourcing of conflict minerals. The Internet has the potential to increase the power of activist groups, thereby making them audible to managers and putting them on an organization's agenda for consideration (Coombs, 1998, 2002; Heath, 1998; T. Putnam, 1993). In 2024, anti-deforestation pressure from Greenpeace resulted in McDonald's pledging to use only deforestation-free products in its global supply chain by 2030. Activist pressure in 2022 forced McDonald's, Coca-Cola, and PepsiCo to suspend operations in Russia over that country's invasion of Ukraine. After first saying it would stay in Russia, Uniqlo reversed the decision and suspended operations in Russia (Cerullo, 2022). Consider how conservative activists in 2024 pressured John Deere, Caterpillar, Harley-Davidson, Molson Coors, and Tractor Supply to cut back or eliminate many diversity, equity, and inclusion (DEI) programs. In 2025, activist pressure caused Amazon and McDonald's to make similar efforts to reduce DEI programs (Riedel, 2025). In 2024, shareholder activists launched 243 campaigns to out chief executive officers (CEOs). They were successful in removing 27 CEOs from their offices, including the CEO of retailer Kohl's (Flaherty, 2025).

The term *cancel culture* has been used to designate a specific type of stakeholder activism that transpires largely within social media. Similar to boycotts, cancel culture centers on withdrawing support triggered by words and/or actions that are deemed inappropriate and that typically involve social justice concerns. Social media is used to call out and to punish the inappropriate or offensive words and actions (Chiou, 2020; E. Ng, 2020). Targets of cancel culture can include organizations as well as celebrities and politicians. The growth of cancel culture is one more illustration of increasing stakeholder activism. Social justice concerns drive many activists. Activists often pressure organizations to act on social justice. Consider how in the spring of 2021, activists pressured organizations to take a stand against Asian hate crimes (Kadrich, 2021). Social justice raises the related concern of social issues. Social issues involve dissensus because there are always at least two conflicting sides. More and more, organizations are expected to take a stand on social issues as well (Arenstein, 2020a; Komiya, 2020). Social issues are difficult because supporting one side can result in the activists on the other side remaining critical of the organization. Overall, there are a variety of factors that all serve to increase stakeholder activism.

Digitization

Our lives are increasingly influenced by digitalization. Whether in our personal lives or at work, we use various digital technologies, including cell phones and tablets. There is a strong reliance on the Internet and its social media platforms for news and communication. The various AI applications are part of this digital milieu in which we live. More and more employers expect employees to use various AI applications, and many people utilize AI in their personal lives too. The term *digital naturals* captures the idea of people utilizing digital technologies (P. Young & Åkerström (2016). Social media has fueled an exponential increase in people being exposed to misinformation and disinformation. Both misinformation and disinformation center on spreading false or incorrect information. The key difference in the intention behind disinformation is lacking in misinformation. Either way, false/incorrect information circulates and can influence people's behavior (Muhammed & Mathew, 2022). During a crisis, misinformation can harm individuals. People might follow advice that is harmful or ignore advice on taking protective action necessary for their safety (Tran et al., 2023). An example is the distribution of aid during a disaster. Misinformation during hurricane Helena resulted in discouraging people from receiving aid and disrupting the distribution of aid when threats were made against aid workers (Gollom, 2024).

Agentic and generative AI can be used to push or even flood misinformation/disinformation messages into the digital environment. Generative AI can create credible looking messages quickly, and agentic AI can be used to distribute those messages at scale. Experts have warned AI can be harnessed to increase the amount of misinformation and disinformation appearing in the digital environment (Saeidnia et al., 2025). The implications for crisis managers can be a distorted view of digital sentiment and public opinion, making it more challenging to identify and interpret indicators of emerging risks.

Broader View of Crises

Prior to the horrific events of September 11, 2001, most organizations were focused on their own little world. Crisis management was driven by what might happen to them on their sites. However, 9/11 showed that attacks or events at other locations can affect any organization. An event does not have to be a major terrorist event to create collateral damage. An explosion at a nearby chemical facility can create a need to evacuate and close an unrelated facility. An airplane crash may prevent vehicles from reaching other offices or plants. Similarly, COVID-19 made managers acutely aware of how a pandemic could affect their operations. A pandemic forced managers to take a more holistic perspective of the world around them.

Consequently, organizations are now broadening their view of crises to include nearby facilities that could create crises for them. Global events have broadened the view of crisis management resulting in an increased emphasis on security and emergency preparedness. Security is one element of prevention and mitigation. Spending and managerial focus on security spiked dramatically after 9/11 and continue to stay high on the list of managerial priorities. While driven by terrorism concerns, security can help with other crises, such as workplace violence. In addition, the security focus has been coupled with the recognition of the need for emergency preparedness. Organizations should be prepared for an evacuation or to provide shelter-in-place, the two basic emergency responses. Emergency preparedness will help organizations with any crisis they face, not just with terrorism (Coombs, 2006b).

Social media has added another layer to broadening the view of crises. Managers are very sensitive to the fact that crisis threats, especially those that damage reputations, can emerge and grow rapidly online. In a study by Burson-Marsteller and Penn Schoen Berland, 55% of managers felt social media had increased their vulnerability to crises (Burson-Marsteller & Penn Schoen Berland, 2011). There is an increasing need to monitor social media and to decide how to integrate it into the crisis response. Later chapters will elaborate on how social media is creating changes in crisis communication. Moreover, organizational participation in the digital world breeds a variety of cybersecurity crises, including data breaches, hacking, and disinformation.

Negligent Failure to Plan

Organizations have long been considered negligent if they did not take reasonable action to reduce or eliminate known or reasonably foreseeable risks that could result in harm. This liability is based on the 1970 Occupational Safety and Health Act (Headley, 2005). The scope of foreseeable risks has expanded to include workplace violence, industrial accidents, product tampering, and terrorist attacks (Abrams, 2005). This new area of liability is known as *negligent failure to plan* and is closely tied to crisis management. Organizations can be found legally liable if they did not take precautions to prevent potential crises and were not prepared to respond. Both crisis prevention and crisis preparation serve as defenses against negligent failure to plan. Juries are already punishing organizations that are not engaging in proper crisis management (Blythe & Stivariou, 2003; Headley, 2005). Crisis management is becoming firmly established as a form of due diligence (efforts to avoid harm to others or to the organization) that will protect an organization not only from the immediate harm of a crisis but from secondary harm resulting from lawsuits.

Employer Duty of Care

In many countries, it is the employer's responsibility to provide a safe work environment that is free of known dangers. Employers must seek to find possible health and safety problems and then take actions to eliminate or to reduce the risks. In the United States, the Occupational Safety and Health Administration (OSHA) regulates the employer duty of care. Employers are required to take actions, including providing training that employees can understand; warning employees of dangers through alarms, labels, color-coded systems, or other means; and ensuring employers have the proper safety equipment and information (OSHA, 2016). Some experts have argued that the employer duty of care extends to employees traveling abroad (Underwood, 2016). Employers must be cognizant of foreseeable risks and take reasonable action to protect employees from those risks. Failures in the employer duty of care can create organizational crises in any organization that has employees. Employer duty of care became more salient during the

COVID-19 pandemic. Organizations had to develop procedures and protocols to enhance the safety of essential workers, such as those in grocery stores and warehouses.

Complexity of Crises

As noted in the introduction, more complex crises are emerging and with greater frequency (Coombs & Tachkova, 2022; Tachkova & Coombs, 2022). All crises are serious, which is why we label the situation a crisis. However, we must recognize some crises are more problematic than others, what we can call sticky crises. Sticky crises are more difficult to manage due to their complexity. This complexity can be a function of the breadth of the geographic areas affects, length of time the crisis transpires, and/or the negative emotions evoked by the crisis (Coombs et al., 2021). The READINESS model of crisis management was created in reaction to the demands exerted by sticky crises. READINESS is defined as "a multidimensional construct with multilevel efficacy, mental adaptability, and emotional leadership-focused mindset, with a dynamic process-driven agility at its core" (Jin et al., 2024, p. 1). See Box 1.2 about READINESS for more information about this new model. The point is there is a need to think about how to address sticky crises in addition to understanding how to manage "regular" crises.

Box 1.2 READINESS Model Overview

The READINESS model has three pillars: multilevel efficacy, mindset, and dynamic process (Jin et al., 2024). Efficacy relates to the ability to complete a task and having that task result in the desired outcome/reaching a goal. Efficacy motivates people to engage with a task and stay with that task—to persevere even when confronting obstacles (Bandura, 1997). READINESS argues efficacy is multilevel. READINESS involves the individual level and two collective levels. The individual level is self-efficacy: Individuals believe they can complete a task and achieve a goal. In a crisis, self-efficacy might be the need to evacuate a building or geographic area. Bandura (1997) noted, "People's shared beliefs in their collective power to produce desired outcomes is a crucial ingredient of collective agency" (p. 65). Collective efficacy is a shared assessment of a group's ability to accomplish their tasks (Chou et al., 2012). The two collective efficacy levels are the crisis team and the organization. Crisis teams must believe they can collectively execute the tasks required to manage the crisis effectively. For the organizational level of efficacy, people must believe the organization will provide the support and resources necessary to manage a crisis properly (Jin et al., 2024).

The right mindset in READINESS relates to crisis leadership with an emphasis on (1) high emotional intelligence, (2) the right attitude, and (3) optimal mentality and adaptability. Crisis communication research has validated the benefits of emotional leadership during the conflict aspect of crisis management (Jin, 2009). Crisis communication leadership requires (a) demonstrating an attitude of organizational leadership in communicating about a crisis and (b) understanding how such an attitude is perceived by stakeholders. Humility, as a type of attitude demonstrated in crisis communication leadership, is critical to managing a crisis as a process in an effective and ethical manner. Humility serves "a sensegiving function that decreases stakeholders' negative emotions and fosters their trust in leadership" (Graffeo & Jin, 2024, p. 1).

Finally, the mindset must capture mental adaptability, one's "ability and willingness to cognitively and affectively adapt to an ongoing situation" (Jin et al., 2024, p. 8) Mental adaptability is composed of four factors: self-efficacy, organizational trust, confidence, and optimism. Crisis communication leaders that can demonstrate optimal mental adaptability are more likely to "(1) believe they can effectively accomplish the crisis tasks required of them (self-efficacy), (2) trust the organization's approach for managing the crisis, (3) be confident in the ability of the organization and its teams to manage the crisis, and (4) be optimistic for the overall outcome" (Jin et al., 2024, p. 8). Leaders need affective and cognitive adaptability when managing crises. Cognitive adaptability requires a leader to focus on understanding the complex situation. Affective adaptability is reflected when leaders withhold individual affective reactions during or after an emotionally charged incident and understanding the nuanced crisis communication situation (Jin et al., 2024).

READINESS is a process driven by a need to adapt to changes in the environment. One cannot be too ready. However, organizations do need to assess the levels of READINESS, making it an outcome too. Assessments are a snapshot in time and a form of outcome. For instance, managers may ask, "How prepared is your organization?" A process view is essential in crisis management. Crises are disruptions for organizations, and disruptions are characterized by uncertainty and change (Obłój & Voronovska, 2024). Sticky crises reflect the disruptive nature of crises. Sticky crises are more complex than regular crises. Strategy becomes more emergent during a crisis as managers read and react to the evolving situation. Managers draw upon the dynamic capabilities of an organization to manage the uncertainty and complexity a crisis might create. Dynamic capabilities are an organization's ability to adapt to changes in the environment—the organization is agile. Dynamic capabilities help managers to navigate uncertainty and disruption (Teece et al., 1997).

Teece et al. (1997) provided a three-step model for utilizing dynamic capabilities. The model was developed to help organizations become more competitive in rapidly changing environments. First is sensing: Managers must locate an opportunity or threat. Second is seizing: Managers must have the capacity to act on opportunities and to take calculated risks. Third is transforming: Managers must be able to reconfigure organizational resources, structures, and process as a continuous process. When dynamic capabilities are applied to crisis management, sensing must focus on threats. Crises are threats to an organization and its stakeholders. All threats are opportunities as well. The opportunity in a crisis is how managers respond to a crisis. A well-managed crisis reflects well upon the organization while a poorly managed crisis further damages how stakeholders perceive and react to the organization (Frandsen & Johansen, 2017). It is appropriate to consider READINESS a form of dynamic capabilities. READINESS is critical for engaging the threat by taking action.

Box 1.3 Crisis Leadership: An Overlooked Resource

Leadership is often overlooked in discussions of crisis management and crisis communication (James & Wooten, 2010). Leadership can be defined as "a process whereby an individual influences a group of individuals to achieve a common goal" (Northouse, 1997, p. 3). During a crisis, leadership can have a major impact on the effectiveness of the crisis management effort. Good leaders regularly are called upon to solve problems, follow plans, and craft visions. These behaviors are all valuable during a crisis. Crisis leadership experts Erika James and Lynn Wooten (2010) argue that crisis leadership is a frame of mind. Good crisis leaders are willing to learn, are open to new ideas, and believe the organization will emerge stronger after the crisis. Crisis leadership is unique because the leaders are being watched by stakeholders (in public view) and are under pressure to utilize shortcuts that will make the crisis disappear but could be ineffective in the long run (James & Wooten, 2010). Each chapter in this book will have a leadership box highlighting various topics relating to effective crisis leadership. Those insights are based on the crisis leadership competencies developed by various crisis management researchers.

Chapter Summary

Organizations are operating in more uncertain environments and are facing more risks and crises than ever before. As the potential for crises increases, so does the potential for negative outcomes. Organizations are playing for high stakes when confronting crises. The developments just reviewed demonstrate that the need for crisis management is increasing, not decreasing. The value of crisis management is greater now than when experts first began preaching about the need for crisis preparedness in the late 1970s. The end result is a higher premium on effective crisis management. Crisis management enhances resilience by increasing the organization's ability to adapt to disruptions. Organizations must continue to improve their crisis management processes. Crisis management acts as a hedge against the negative outcomes of crises and facilitates resilience. Effective crisis management can protect lives, health, and the environment; reduce the time it takes to complete the crisis life cycle; prevent loss of sales; limit reputation damage; preclude the development of public policy issues (i.e., laws and regulations); and save money. Today's operating environment demands that organizations be prepared to manage crises.

Generally, we experience crises through the news media and the Internet. As a result, it is easy to view crisis management as a short-term process and crisis managers as having few demands on their time. However, what the public sees of the response to a crisis is a small part of crisis management. Effective crisis management is ongoing. Crisis managers continually work to reduce the likelihood of a crisis occurring and to prepare the organization for the day when a crisis does occur, thereby increasing adaptability and resilience for the organization and its stakeholders. Moreover, crisis managers carefully dissect each crisis in order to improve mitigation, preparation, and response. An appreciation of the phases of crisis management helps people to understand more fully the complexity and ongoing nature of crisis management and communication. The increasing complexity of crises makes crisis management more challenging. AI is one of the factors shaping the new, more complex crisis management environment. It is important to understand how the various types of AI contribute and help to navigate the increasingly complex crisis dynamic.

Discussion Questions

1. What are some arguments managers would use against implementing a crisis management system?
2. Do you agree or disagree with the idea that a crisis is perceptual?
3. What do you think makes an event a crisis? How do crises differ from disasters?
4. What alternatives are there to a staged approach to crisis management?
5. Some people question the value of precrisis activities. What reasons do you see that argue for and against precrisis activities?
6. Why bother differentiating between crises and paracrises?
7. What does the regenerative crisis model add to the thinking about crisis management?
8. How would you justify adding a crisis management program to an organization?
9. Why is stakeholder activism likely to increase as a concern for crisis managers?
10. What are the implications of crises are becoming more complex?
11. What are some of the ways you anticipate the various AI applications to affect crises and crisis management?
12. How is the READINESS model a new approach to crises?

Chapter 2

Risk as the Foundation for Crisis Management and Crisis Communication

Chapter Objectives

- Explain the different categories of risk in the knowns and unknowns framework of risk.
- Identify the different types of risks found in organizations.
- Describe the key elements of enterprise risk management.

The best way to manage a crisis is to prevent one. If the crisis does not occur, no stakeholders are harmed and the organization suffers no damage. Generally, people think of crisis management as reactive because they focus on what an organization does in response to a crisis, which is the topic of Chapter 7. However, clever crisis managers are proactive because they seek crisis warning signs and take measures designed to reduce or eliminate the possibility of the warning sign evolving into a crisis—crisis managers seek to identify and cope with risks. In the digital age, crisis warning signs are abundant, if crisis managers can find and interpret them effectively. I feel it is critical to understand how risk is the foundation for crisis communication. Risk is intricately linked with resilience as well. Risk and resilience share a proactive nature, provide options for dealing with shocks, and focus on the ability to manage disturbances.

One technical definition of *risk* is "uncertainty about and severity of the consequences (or outcomes) of an activity with respect to something that humans value" (Aven & Renn, 2009, p. 1). More generally, we can think of risk as the potential to do harm. For organizations, risk centers on the threat or probability that a vulnerability creates loss, damage, or injury. The term *threat* implies opportunity as well. A situation is a threat or an opportunity depending on the response (Churning, 2025). Threat and opportunity are a duality, not a binary by nature. A risk is a threat if it develops but is an opportunity if managed properly. A risk is the knowledge that something bad can happen while a crisis is when something bad has happened. Simply put, a crisis can arise when a risk is realized.

Every organization faces a variety of risks but have different views of and levels of risk acceptance. Organizations have specific risk appetites, the amount of risk an organization is willing to take in pursuit of its objectives. Organizations also have risk tolerances, the maximum risk an organization is willing to accept for a specific task. Organizations can vary in their risk appetites and risk tolerances. Moreover, risk tolerances can vary from task to task in the same organization. While having a general risk appetite, managers may be willing to accept more or less risk for a specific task (risk tolerance) (Marks, 2011).

The global importance of risk is reflected in the many annual reports that provide insights into the top risks managers will face. Those producing annual risk reports include Alliance and AXA (insurance companies), KPMG and Deloitte (consultancies), Aon, and the World Economic Forum. While the lists are useful, we need to consider how managers can think about and organize risks. This chapter begins with a broad categorization of risks based upon the ideas of knowns and unknowns first suggested by then U.S. Secretary of Defense Donald Rumsfeld. The chapter then moves deeper into the organizational context by exploring three specific categories of organizational risks and ends by exploring the integrative framework of enterprise risk management.

The Knowns and Unknowns Framework of Risk

In 2002, Donald Rumsfeld gave an answer in a press conference talking about known-knowns and unknown-unknowns. At the time it seemed like he was just trying not to answer the question, but risk experts later embraced this knowns-unknowns distinction for risks. The knowns and unknowns framework of risks is built upon the two dimensions of recognition of risk and insights into risks. Each dimension has two categories, knowns and unknowns. The dimensions and categories create a 2 × 2 matrix of known-known, known-unknown, and unknown-known, and unknown-unknown.

Recognition of risks are those risks managers will acknowledge as important. Known risks are those risks managers "see" while unknown risks are unseen either through lack of information or a choice to not see them. Insights into risks reflect the quantitative or qualitative nature of risks. Quantifiable risks have numerical values placed on their occurrence; for example, the odds of an airliner crashing is 1 in 11 million. Qualitative risks lack quantifiability (Stoel et al., 2017). For instance, we cannot put a number on the odds of a CEO being forced to resign after being caught on camera at a music concert with someone who was not their spouse. This inability to place a number on them makes qualitative risks unknown because you cannot have many insights into these risks but you realize they do exist.

Known-knowns are risks managers recognize and have a lot of information about and insights into the risks. Known-knowns are the heart of crisis management efforts because these are risks managers are familiar with and deal with on a regular basis. For instance, companies in the food industry realize the risk of foodborne illnesses, petrochemical companies realize the danger of hazardous chemical releases, and those in transportation realize the risk of accidents. Organizations are thinking about the known-known risks. Known-unknowns are the qualitative risks managers recognize as possible but have little information about (lack of insight). Examples would be scandals from management misconduct and a sudden spike in negative comments on a social media platform. Managers can anticipate the known-unknowns but have minimal insights into them.

Unknown-knowns are an odd category. How can a risk not be recognized when there is abundant knowledge about it? The answer is what psychologists call willful ignorance. Willful ignorance is when people choose to ignore something like a risk and are not simply overlooking the risk (L. Vu et al., 2023). Unknown-knowns have also been called gray rhinos (Wucker, 2016). It is a purposeful attempt to ignore a risk that potentially could manifest into a crisis, making willful ignorance problematic when managing crises. Managers are choosing not to address a risk they could understand. Consider how bad willful ignorance will look after a crisis when stakeholders learn managers ignored the risk. This should increase the reputational damage the crisis inflicts upon the organization and raise questions about the organization's culture and governance. It is what some refer to as the optics being bad. A poignant example is the COVID-19 pandemic. Managers knew for decades a pandemic was possible. There was information about this risk, yet most organizations ignored it. Unknown-unknowns are risks we do not see because we know little or nothing about them. These are shocks when they manifest into crises, what are often called black swan events. Unknown-unknowns produce unique events people could not have anticipated or had difficulty anticipating.

The knowns and unknowns framework of risks is not a precise list of specific risks. Rather, the framework is a way to think more broadly about risks and the risks an organization is seeking to understand and to address and those they are not. The framework provides one way of determining blind spots in an organization's approach to risk that can impact crisis management. I will refer back to this knowns and unknowns framework of risks in the discussion of preparation in Chapter 4.

Risk in the Organizational Context

While concepts in this book can be applied to crisis management in general, the primary focus is on the organizational context. To appreciate the organizational context of risk, it is instructive to consider the unique forms of risk managers face. This section examines three risks critical within organizations: stakeholders as risk, issues management as risk management, and reputation and risk.

Stakeholders and Risk

Stakeholders fit with the discussion of risk because stakeholders are a source of risk for organizations. For instance, activists can create a risk by creating negative publicity or social media discussions about an organization. Moreover, organizations can create risks for stakeholders. The release of a hazardous chemical by an organization, for instance, can place employees and the community at risk. Stakeholder mapping identifies the stakeholders relevant to the organization. Stakeholder mapping is one approach in risk management used to identify the risks associated with the various stakeholders. The point is that understanding stakeholders informs enterprise risk management and how to understand organizational risks. The discussion of stakeholders begins by clarifying their relationship to risk then considers how stakeholders help to create paracrises, a specific form of crisis risk.

Stakeholder theory is one way to think about the various constituents that are somehow connected to and affect an organization. Various people and groups share stakes, some connection, to an organization. Stakeholder theory posits that an organization's environment is populated with various stakeholders. An organization survives or thrives by effectively managing these stakeholders (Bryson, 2004; Clarkson, 1991; Wood, 1991). Stakeholders are generally defined as any persons or groups that have an interest, right, claim, or ownership in an organization. Stakeholders not only have an interest in the organization but can affect or be affected by the organization (Freeman, 1984). Stakeholders can be separated into two distinct groups: primary and secondary. Primary stakeholders are those people or groups whose actions directly affect (can be harmful or beneficial to) an organization. Failure to maintain a continuing interaction with a primary stakeholder could result in the failure of the organization. Typical primary stakeholders include employees, investors, customers, suppliers, and the government. For instance, organizations cannot operate without employees, and government officials may close a facility for a variety of legal or regulatory reasons. Secondary stakeholders or influencers are those people or groups that have an indirect influence on organizations but can still affect or be affected by the actions of an organization. Typical influencers include the media, activist groups, and competitors. Influencers cannot stop an organization from functioning, but they can damage it (Clarkson, 1995; Donaldson & Preston, 1995).

Primary and secondary stakeholders are interdependent with an organization; thus we talk about *organization–stakeholder relationships*. Each of the stakeholders has a connection (stake) with the organization that links them in some way. Stakeholders can have relationships with one another as well. Moreover, stakeholders may have competing demands, which creates conflicts between themselves and the organization. Organizational success is predicated on maintaining an effective balance in these relationships (Donaldson & Preston, 1995; Rowley, 1997; Savage et al., 1991). It follows that stakeholders can play an important role in crisis management.

Primary stakeholders can stop organizational operations and trigger a crisis. Conflict with an organization can lead primary stakeholders to withhold their contributions. As a result, an organization may stop operating if those contributions cannot be replaced. For instance, unhappy workers can strike, and discontented customers can boycott. In 1997, the Teamsters' 15-day strike against UPS cost the company $600 million in revenues. A total of 185,000 Teamsters, nearly two thirds of the UPS American workforce, joined the strike. At best, UPS was able to operate at only 10% capacity, using management personnel and drivers who did not strike. UPS found it could not function without the drivers, so it conceded to their demands (Sewell, 1997).

Sonos is an audio company that specializes in home speakers, including multi-room audio systems. Their customers clearly value audio quality and could be considered audiophiles. On May 7, 2024, Sonos released an extensive software update for its app. Customers quickly began to complain about serious problems, including vanishing playlists, smart speakers being useless, and inaccessible music libraries. The complaints were being posted online to various forums, including the Sonos Community. These are very serious concerns for audiophiles. Initially Sonos showed no concern about their customers' problems. The company defended the update by saying, "It takes courage to rebuild a brand's core product from the ground up" (Clover, 2024, para. 4). The complaining customer posts only increased following the company's initial statement and lack of responsiveness and engagement with customers. On July 25, 2024, Sonos CEO Patrick Spence posted a message online that started by saying, "We know that too many of you have experienced significant problems with our new app which rolled out on May 7, and I want to begin by personally apologizing for disappointing you" (Spence, 2024, para. 1). The message went on to validate the concerns of customers and began to seriously engage with customers and their problems. However, the damage had been done, as Sonos lost approximately $100 million dollars in revenue and $500 million dollars in market value (Nickinson, 2024). Primary stakeholders are powerful because it is difficult and often impossible to replace the contributions they provide to the organization (R. K. Mitchell et al., 1997). For crisis management, it would be a mistake to focus solely on primary stakeholders. Problems in relationships with secondary stakeholders can also harm reputations and trigger crises. The media can expose organizational misdeeds or generate other negative publicity, competitors can instigate lawsuits that bind an organization's operations, and activists can launch boycotts or protests against an organization. A few examples illustrate the role of secondary stakeholders in creating crises.

On July 28, 2022, the Consumer Financial Protection Bureau concluded a five-year investigation into U.S. Bank with a $37.5 million dollar fine. For over a decade the company had been unlawfully accessing the credit reports of customers and using the information to open sham accounts and new lines of credit. The actions were taken to inflate sales number because of the internal pressure being placed on U.S. Bank employees to boost numbers. Many of the customers suffered damaged credit profiles. Management at U.S. Bank had been aware of the practices of creating fake accounts for years but ignored it (Tangalakiz-Lippert, 2022). A government investigation exposed the crisis and it then was covered widely by the media.

Trademarks are important to organizations because customers often recognize a brand through its trademark. Organizations legally file for trademarks and keep them by protecting it through filing lawsuits against those who would violate it. In 2022, Jack Daniel's sued VIP Products over a dog chew toy sold by the company. The dog toy was shaped like a Jack Daniel's whiskey bottle. The label read "Bad Spaniel" and "Old No. 2 on Your Tennessee Carpet." VIP Products argued it was legal because it was parody, a class of protected speech. An appeal court ruled against VIP Products claiming they used the Jack Daniel's trademark as a trademark, and that is a violation of trademark law (*Jack Daniel's Properties, INC v. VIP Products LLC*, 2023).

In both cases, a secondary stakeholder had influenced organizational actions. Secondary as well as primary stakeholders can create a crisis for an organization. Mismanaging the organization–stakeholder relations can evolve into a crisis (Grunig, 1992; Heath, 1988). Therefore, watching organization–stakeholder relationships contributes to crisis scanning. Early problems in an organization–stakeholder relationship might be a sign that a crisis could erupt.

Chapter 1 introduced the paracrisis as a distinct form of crisis risk to differentiate such situations from operational crises. Paracrises center on the public management of a risk. Managers must address or ignore the risk as stakeholders watch. There are six types of paracrises: faux pas, challenge, guilt by association, misinformation, social media misuse, and social media account hacking (F. Chen & Holladay, 2023). Organizations, like people, can do things intended to be good but end up embarrassing them—committing a faux pas. There are two variations of the faux pas paracrisis. First, managers execute an action they think will be positive but at least some stakeholders view as negative. An example would be some customers being offended by the content of an advertisement intended to boost sales. Second, managers unintentionally allow someone to create offensive or insensitive content that is attributed to the organization. People might post content to an organization's social media account that is offensive, and that offense is then linked to the organization.

The challenge paracrisis occurs when some stakeholders argue that existing practices of an organization are irresponsible or simply wrong in some way. A typical example of a challenge paracrisis is when some stakeholders claim an organization is sourcing raw materials in an irresponsible manner or engaging in practices that are harmful to society. Consider how some luxury brands were criticized for using sandblasting techniques to distress clothing, thereby placing worker health at risk with the practice. Guilt by association involves some negative actor or action being linked to an organization. Often a spokesperson linked to an organization engages in troubling behavior. Some of the negativity associated with that spokesperson transfers to the organization. Box 2.1 presents more details about "brand safety crises," a distinct form of guilt by association. The misinformation paracrisis involves unverified and negative information about the organization being circulated among stakeholders. For decades P&G has faced misinformation linking the company to Satan worshiping. The digital world has increased the frequency of misinformation paracrises (Tuttle, 2021).

Box 2.1 Brand Safety Crises

Brand safety crises are not about product harm; rather, they are about being associated with negative digital content. As brands utilize more social media platforms to convey content, there is a risk their messages will appear in close proximity to other messages that are deemed toxic content, such as vulgar language, hate speech, pornography, and violent images. Proximity to such toxic content can damage a brand. This situation is called a brand safety crisis. In 2019, a survey of marketing professionals found that 60% were concerned about brand safety crises (Schraeder, 2019). Using the term *crisis* is imprecise; the situation is more of a paracrisis (guilt by association) than an operational crisis because it is about managing a risk. Still, the brand safety paracrisis is a threat that crisis managers must consider.

Social media misuse is when stakeholders identify that the organization has violated social media rules or ethos. Using hashtags designed to help people during a disaster to sell clothes is an example of social media misuse. Social media account hacking is when an organization's social media account is hacked and others maliciously post information damaging to the organizations. Hackers once hijacked Burger King's Twitter (now X) account and posted information about employees engaging in illegal activities (Chen & Holladay, 2023).

The digital naturals and the digital world make paracrises more likely to occur because it is so easy for stakeholders to share information. Moreover, all six types of paracrises are driven by stakeholders in some way. Stakeholders either initiate the paracrisis with their actions (sharing misinformation or hacking an account) or identify the situation as problematic (challenge behavior, identify a faux pas, make the link to a negative actor, and note the misuse of social media). Stakeholders are the reason managers need to be aware of and to manage paracrises. Paracrises often reflect affective polarization too.

Affective polarization emphasizes the divisions within a society and is a global concern. Affective polarization occurs when opposing groups distrust and dislike one another (Castle & Stepp, 2021). It is about antagonism between the sides that shapes interactions. People are interested more in their difference than solving a conflict—it is a highly contentious environment (USC, 2022). Social issues are a common trigger for affective polarization because social issues are naturally divisive (Coombs & Holladay, 2018). Social media outlets add fuel to the division by providing platforms for attacking the opposition and promoting one's own positions (Kubin & Von Sikorski, 2021). Affective polarization is dysfunctional when it breeds intolerance, a general rejection of values and practices different from one's own. Polarization embodies both intuitive (disapproval of values and practices of others) and deliberative (the position that the views and values of others cross a boundary of what is acceptable and violate one's own moral principles) intolerance (Verkuyten et al., 2020). The rise in affective polarization is another factor sure to increase the number of paracrises managers will face. Polarization is relevant to issues management as well.

Issues Management

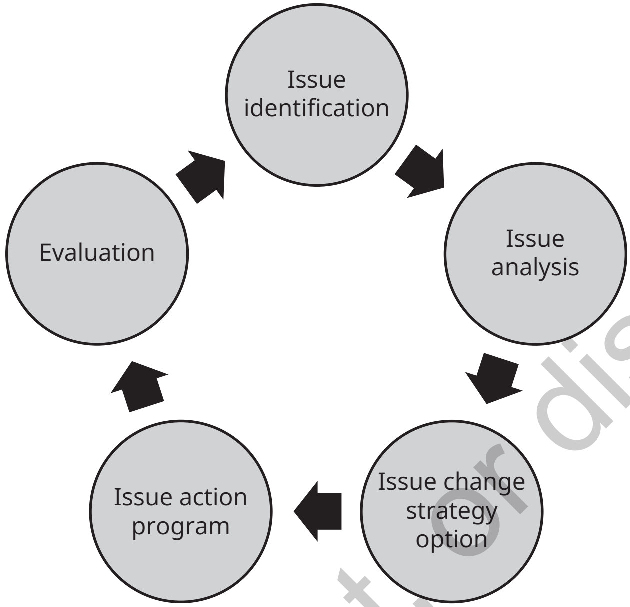
An issue is "a trend or condition . . . that, if continued, would have a significant effect on how a company is operated" (R. H. Moore, 1979, p. 43). In essence, an issue is a type of problem whose resolution can impact the organization. Issues management includes the identification of issues and actions taken to affect them (Heath, 1990). It tries to lessen the negative impact of an issue and is a systematic approach intended to shape how an issue develops and is resolved. Issues management is a proactive attempt to have an issue decided in a way that is favorable to an organization. While issues management can address internal concerns (Dutton & Jackson, 1987; Dutton & Ottensmeyer, 1987), the emphasis is on societal and political issues that populate the organization's environment—external issues (Heath, 2005). Issues can create risks for organizations that emerge within the organization's environment. Hence, managing an issue can be a specific form of risk management. The early work in issues management concentrated on governmental decisions such as legislation and regulation. At the end of this section the expansion of issues management into social issues is considered.

Managing an issue involves attempts to shape how the issue is resolved. The idea is to have the issue resolved in a manner that avoids a crisis. For instance, say that legislation is proposed that would threaten the financial viability of the railroad by making trucking companies more competitive with rail transportation. The issues management effort prevents a crisis by persuading Congress to reject the legislative proposal. Communication is used to influence an issue's resolution.

The Jones and Chase (1979) model (issue identification, analysis, change strategy option, action program, and evaluation) is the classic model familiar to most people involved in issues management. The action step centers on communicating the organization's position on the issue to stakeholders involved with the issue. Goals and objectives for the communication program are developed, followed by the selection of the means and resources needed to achieve them. Decisions are made about the specific messages to be communicated, when to communicate them, and the channels of communication to be used (Jones & Chase, 1979). The exact mix of communication strategies depends on the stakeholders involved in the issues management effort and the current stage of the issue's progression (Crable & Vibbert, 1985). Developing the previous transportation example can clarify the issue action program. The railroad company decides the goal is to prevent passage of the pro-trucking legislative proposal. Legislators, the media, and voters are the stakeholders to be targeted. The message centers on the danger to automobile drivers created by the pro-trucking legislation, and the message must be sent immediately because a vote will be held in a few months. Advertisements, publicity, and lobbying are the communication channels used. The focus in this example is on how organizations use issues management to shape their environments. Figure 2.1 is a visual depiction of the Jones and Chase model.

Issues management can also involve changing the organization. Issue managers may decide that the best way to resolve an issue would be to correct or improve operating standards and plans. McDonald's illustrated this point when it abandoned the polystyrene "clamshell" burger boxes. Environmentalists had been complaining about the environmentally unfriendly clamshell packaging for years. The company's original plan was to win acceptance of the clamshell by emphasizing recycling. By recycling, McDonald's would eliminate the complaint that its packaging would clog landfills for hundreds of years. McDonald's was trying to change stakeholder attitudes. However, consumers did not respond well to the early recycling tests, so McDonald's abandoned the clamshell recycling campaign and simply ended use of that packaging (A. Snyder, 1991). McDonald's changed its procedures rather than trying to change its stakeholders' opinions. As Gonzalez-Herrero and Pratt (1996) note, some issues can develop into crises, making issues management relevant to crisis scanning. Issues management can be a form of crisis prevention when the issues management effort prevents an issue from developing its crisis potential (Grunig & Repper, 1992). An example of this is pharmaceutical companies' use of direct-to-consumer (DTC) advertising. You have no doubt seen many DTC messages. Have you seen television advertisements for drugs to address cholesterol, high blood pressure, social anxiety, acid reflux, or sexual dysfunction? Then you have been exposed to DTC. The United States and New Zealand are the only developed countries to allow DTC efforts. In 2018, Purdue Pharma began an effort to address the growing concerns over opioid abuse in the United

Figure 2.1 ▪ Jones and Chase Issues Management Model



Source: Jones & Chase, 1979.

States. Purdue Pharma is intricately linked with opioids in the United States because the company was highly successful in introducing its opioid drugs in this country and helped to popularize their use. Purdue Pharma began supporting efforts to reduce the length of a patient's first opioid prescription and working to create opioids that had "abuse deterrent properties" (Purdue Pharma, 2017, para. 3). Purdue Pharma then took a more dramatic action by announcing it would no longer market opioids to doctors and would cut its sales force by 50% (Schott, 2018). These actions were designed in part to forestall potential regulatory actions being taken against opioid manufacturers. Purdue Pharma was trying to demonstrate the industry could self-regulate, making governmental intervention unnecessary—Purdue Pharma was trying to manage the opioid issue.

A crisis or ineffective crisis management can spawn an issue, creating the need for issues management. After its introduction, the Boeing 737 Max airliner was involved in two deadly crashes, and use of the aircraft was grounded and could not be flown from March 2019 to December 2020. The crashes were the impetus behind the 2020 Aircraft Certification, Safety, and Accountability Act, which created significant reforms of how the Federal Aviation Administration (FAA) in the United States certifies aircraft and increased the FAA's oversight over aircraft manufacturers like Boeing. In 2020, German fintech company Wirecard announced it was missing 1.9 billion euros. Closer inspection found the nearly 2 billion euros did not exist because Wirecard had been inflating its cash balances and profits for years. It was dubbed the German "Enron." In June 2020, Germany adopted the Act of Strengthening the Financial Market Integrity, which established new requirements for corporate governance. The changes included requiring all listed and public-interest entities to have a mandatory audit committee and rules for the composition of that committee (Browne, 2020).

Sometimes issues can be used to create an advantage for some actors in an industry and a disadvantage for other actors. Airbnb and other online, short-term rental platforms have presented a problem for the hotel industry. In New York City, the Hotel Association of New York City (HANYC) and the American Hotel and Lodging Association (AHLA) worked to pass what is called Local Law 18 (aka the Short-term Rental Registration Law) in 2022 and the law began being enforced in 2023. Local Law 18 was presented as an effort to help ease the housing shortage in New York City by reducing the number of apartments being used for Airbnb rather than for regular housing. Local Law 18 requires any rental properties renting for under 30 days to be registered with the city's Office of Special Enforcement (OSE). In addition, no more than two people can stay in the unit, the unit can only be part of a dwelling not the entire dwelling, and the hosts have to be onsite during the rental period. The result was a crisis for Airbnb because of a significant drop in Airbnb rentals and listings in New York City. This crisis was the desired outcome for the hotel industry because hotels gained an advantage by decreasing competition (Radich, 2024).

Issues management has been expanding beyond governmental decisions for years. Heath (2005) noted this change in how he altered his definition of issues management to no longer include a focus on governmental decisions. Coombs and Holladay (2018) use the term *social issues management* to capture the nongovernmental component of issues management. Social issues are societal concerns that are polarizing because people will take at least two different positions on the issue (Global Strategy Group, 2016). With social issues, the organization rather than some government entity is the decision maker. Managers decide to make changes to policies and behaviors and are not required to do so by government mandates. When Greenpeace convinced Nike and Puma to stop using certain toxic chemicals in clothing manufacturing, that was social issues management. Greenpeace used a variety of communication channels to pressure the two companies into changing their supply chains.

Activists use social issues management to pressure companies to change. The activists use communication to connect a company to a social issue and generate negative publicity and word-of-mouth about the organization being on the "wrong side" of the social issue. If the leverage is strong enough from the communication efforts and the cost of the change is low enough, the company will change its position on the social issue (Coombs & Holladay, 2018). Managers must be cognizant of stakeholder efforts designed to manage social issues by pressuring the organization to change. One example of that is the challenge paracrisis. The challenge argues the organization is acting socially irresponsible. A challenge can be instrumental to the stakeholder's social issues management effort.

The emergence of social issues management reflects the growing sociopolitical context that expects companies to take action on social issues (Arenstein, 2020a; Komiya, 2020). Polling data and surveys indicate stakeholders overwhelmingly want companies to take stands on sociopolitical issues (e.g., Edelman, 2023; USC, 2022). This type of data puts pressure on managers to engage in what is called corporate social advocacy (CSA). CSA "refers to an organization making a public statement or taking a stand on social-political issues" (Dodd & Supa, 2014, p. 5). CSA fuses issues management and corporate social responsibility (CSR) and is the most recent step in the evolution of corporate advocacy (Coombs & Holladay, 2018). Managers need to step back and look at the bigger picture. Yes, stakeholders want companies to take stands on sociopolitical issues, but stakeholders want companies to take stands consistent with their views of issues. Sociopolitical issues always have at least two sides. Even if 80% of stakeholders want a company to take a stand on an issue like same-sex marriage, not all stakeholders want the company to take a stand to support or to oppose it. This is when polarization matters. Sociopolitical issues are polarizing (Coombs & Holladay, 2018); hence, taking a stand on one will invite both praise and condemnation. The key takeaway is that managers must be aware of social issues relevant to their industries and how their stance on a social issue (or lack thereof) can result in the organization being drawn into a paracrisis or even a crisis (Coombs et al., 2021).

Reputational Risk

A reputation is an evaluation stakeholders make about an organization. Hence, we can talk about favorable and unfavorable reputations. Reputation is a form of social evaluation stakeholders make about organizations (Pollock et al., 2019). Social evaluations, such as reputation, create social approval assets and liabilities (Bundy & Pfarrer, 2015). More generally, a favorable reputation is a social approval asset while a negative reputation is a social approval liability. Reputation, and social evaluations in general, can be damaged by failing to meet stakeholder expectations related to climate change, sourcing products in an irresponsible manner, having to recall a product that has harmed customers, or any situation that generates negative media coverage for the organization. Risk managers are increasingly interested in reputational risks (social evaluations). For instance, Allianz's (2021) Global Risk Dialogue white paper centered on reputational/social evaluations risks. As noted in Chapter 1, positive reputations are widely recognized as a valuable yet intangible asset and are one form of social evaluation made by stakeholders. This chapter highlights reputational risk because organizations recognize it as a unique form of risk. However, the same points apply to any form of social evaluation by stakeholders. How managers report reputational risks in their 10-K reports (discussed later) illustrates the importance attached to this form of risk.

Reputation risk is recognized by corporate leaders as a critical risk. AON's (2019) Global Risk Management Survey identified reputational risk as a top five risk for executives. Reputational risks are linked to crises and the media coverage from crises that produce financial losses. "Whenever a business undergoes a reputation event it cuts to the core of their brand's perception. And the combination of our 24/7 news cycle with widespread use of social media puts brands at risk for long-term negative consequences, both in public perception and in the marketplace" (AON, 2019, p. 24). Reputational risks are uniquely dangerous because they can appear with little or no warning. Allianz's (2020) Risk Barometer placed loss of reputation as number eight on its 2020 Top 10 Global Business Risk list. Moreover, Deloitte (2018) noted that reputational risks are difficult "to define and quantify" (p. 53). Reputational risks are part of the challenging nonfinancial risks. Deloitte (2018) found that 39% of executives identified reputational risk as an important risk while just 57% were confident their organization can manage such risks. Conduct risks can be treated as a form of reputational risk. A conduct risk is when managers engage in misconduct that harms employees, customers, and/or the reputation. Organizations often "find it challenging to manage conduct and culture risk" (Deloitte, 2018, p. 62). This difficulty results in conduct risks often being overlooked in risk management programs. The point is the conduct risks should be part of reputation risk element of the enterprise risk management process.

To understand reputational risk, we must start by understanding how reputations are formed. Reputations are formed as stakeholders evaluate organizations based on direct and indirect interactions. Direct interactions form the basics of the organization–stakeholder relationship (Fombrun & van Riel, 2004). Positive interactions build favorable reputations, while unpleasant interactions lead to unfavorable ones. Favorable stakeholder relationships can be taken as a marker of a positive reputation. The relationship history—how the organization has treated stakeholders in the past—is a function of an organization meeting or failing to meet stakeholder expectations (Finet, 1994). Organizations build favorable relationship histories that create positive reputations by meeting and exceeding stakeholder expectations (Coombs, 2004a).

Indirect interactions are mediated reports of how the organization treats its stakeholders. News reports, comments from friends or family, online comments, and messages sent by an organization are important sources of information for evaluating organizations. Do you dislike Enron? Did you meet anyone from Enron, buy Enron stock, or purchase products from Enron? The odds are that you built your opinion of Enron based on media reports. In fact, stakeholders are more likely to draw on indirect than direct experiences when crafting their personal views of an organization's reputation (Carroll & McCombs, 2003; Stephenson & Blackshaw, 2006). Being evaluative, reputations are based in large part on how stakeholders assess an organization's ability to meet their expectations. How well an organization does this is a rough guide for determining whether a reputation will be positive or negative. In some respects, a reputation is a reflection of the organization–stakeholder relationship. A threat to the relationship is a threat to the reputation. It is important to dig deeper into the relationship to appreciate its connection to reputations.

But what does the term *relationship* mean? Talking about organizational relationships with stakeholders assumes that we all understand and agree on what is meant by *relationship* and *stakeholder*. For crisis management, a useful definition of relationship is the interdependence of two or more people or groups. This definition is a modification of one developed by O'Hair et al. (1995) and centers on interdependence, some factor that binds the two people or groups together. The interdependence definition of relationship is useful because it is consistent with the stakeholder theory that guides most business thinking (Rowley, 1997).

The broadening array of stakeholders that are important to organizations has promoted the integration of corporate social responsibility (CSR) into the conceptualization and management of reputations. CSR can be defined as "the management of actions designed to affect an organization's impacts on society" (Coombs & Holladay, 2010, p. 262). The societal impacts of CSR are quite diverse, including worker rights, sustainability, human rights, and eradication of disease. Traditionally, financial factors have dominated corporate reputation management. The financial factors became the criteria used to evaluate corporate reputations. The dominant reputation measures, such as *Fortune* magazine's Most Admired list and the Reputation Institute's RepTrak (originally the Reputation Quotient), reflect a financial orientation. Social responsibility has been a more minor element within these measures. For instance, the RepTrak has seven dimensions: leadership, performance, products and services, innovation, citizenship, workplace, and governance. CSR is a part of citizenship (e.g., contributes to society), workplace (e.g., cares about employee well-being), and governance (e.g., responsible use of power) dimensions. The Most Admired list has eight dimensions, with only one—community and environmental responsibility—relevant to CSR.

CSR increasingly is playing a more important role in reputation discussions. Charles Fombrun (2005), a leader in reputation management thinking, now refers to CSR as an integral aspect of reputation. CSR is quickly becoming a key driver and integral part of reputation management. Reputations are evaluations and can range from favorable to unfavorable. Both CSR and reputation are dependent upon stakeholder expectations. In fact, the current thinking in CSR is that stakeholder expectations are the foundation for the process. Stakeholders define CSR by determining what social concerns are appropriate for CSR efforts (e.g., Bhattacharya & Sen, 2003; Coombs & Holladay, 2010). Reputation managers can no longer concentrate exclusively on investors and their financial interests. CSR now is part of the key evaluation criteria for reputations and comprises over 40% of an organization's reputation (J. Smith, 2012).

Crisis managers must now consider CSR activities as a form of crisis risk. CSR activities generate three distinct forms of reputation risk. The first risk is greenwashing. Greenwashing occurs when an organization's environmental claims are shown to be false (Coombs & Holladay, 2015a). The reputation is harmed when the organization is shown to be hypocritical. The second risk is that engaging in CSR makes organizations more vulnerable to reputational attacks related to irresponsibility. When an organization publicly engages in CSR, the organization is claiming to be socially responsible and makes social responsibility a part of its reputation. If stakeholders can successfully argue the organization is socially irresponsible, there is greater potential of damage to the organization's reputation than if the organization had not engaged in CSR. Engaging in CSR creates a unique form of crisis risk (Coombs, 2017a; Coombs & Holladay, 2015a). For instance, H&M engages in CSR and uses CSR as a key part of its reputation. When Greenpeace claimed H&M was socially irresponsible for allowing the use of toxic chemicals in its clothing supply chain, H&M quickly changed that practice (Coombs, 2014). The change was necessary to protect the social responsibility aspect of H&M's reputation. H&M was vulnerable to Greenpeace's social irresponsibility attack because H&M had a public commitment to social responsibility. A company that does not commit to CSR will not have that same vulnerability. Engaging in CSR creates a vulnerability to challenges from stakeholders that the organization is acting irresponsibly.

The third risk is when CSR activities trigger a paracrisis or crisis. In the early 2020s, CSR as risk took a new twist. Greenhushing began to emerge. One variant of greenhushing is when corporations engage in environmental activities but choose not to promote those activities as they had done in the past. It had become a risk to talk about efforts to reduce a corporation's contribution to climate change because activists were attacking corporations for such actions (Haigh & Liszka, 2024). Slowly the attacks on what were previously considered positive CSR actions expanded to include many social concerns such as DEI (McCauley, 2024). As noted early in this chapter, conservative activists pressured corporations to decrease or to drop DEI initiatives. Essentially CSR was blending with CSA (Hydock et al., 2020). Because many activists chose to politicize CSR efforts (frame them as political concerns), many CSR efforts were now viewed as CSA efforts, creating yet another variant of CSR risk.

As noted earlier in this book, crises have a negative effect on reputations, turning a social approval asset into a social disapproval liability. Reputations also have an effect on crisis management. A negative reputation prior to a crisis makes the crisis more difficult to manage. A prior negative reputation, for instance, increases stakeholder perceptions that the organization is responsible for the crisis and increases reputation damage (Coombs & Holladay, 2002, 2006). A positive reputation prior to a crisis acts as a resource that can make crisis management easier. Crisis experts agree that favorable organization–stakeholder relationships are a benefit during crisis management (e.g., Ulmer, 2001). As Alsop (2004) states, organizations "build up 'reputation capital' to tide them over in turbulent times. It's like opening a savings account for a rainy day. If a crisis strikes . . . reputation suffers less and rebounds more quickly" (p. 17). A crisis will inflict some reputation damage on an organization. "A crisis or other negative development will certainly tax any reputation and rob a company of some of its stored-up reputation capital" (Alsop, 2004, p. 17).

Modern organizations face a wider array of reputational risks when CSR and social media are added to the mix. The earlier discussion linked CSR to reputation. Increasingly, CSR is becoming a risk because of its importance to reputation. If an organization is shown to be irresponsible, such as in a challenge paracrisis, the reputation is damaged. Hence, CSR becomes a risk for the organization. For instance, organizations manage CSR risk by auditing their suppliers to determine whether the suppliers are meeting the organization's code of conduct regarding social and environmental issues. While organizations turn to social media to build relations with other stakeholders, these channels and platforms are risks as well. Stakeholders can hijack social media (control the content of the messages) and damage an organization's reputation. The utilization of social media platforms is a risk that must be managed. CSR and social media risks illustrate the complex nature of reputational risks.

At this point it is helpful to reinforce the qualitative nature of reputational risks, making them a form of known-unknown risk. Debanking illustrates the qualitative and variable nature of reputational risks. Debanking is when a bank closes a client's existing account or refuses to open an account for a potentially new client deemed risky. One part of the risk was the potential for criminal activity within the industry of the potential client. Cryptocurrency and cannabis companies are frequent targets of debanking. The other part of being risky is the potential reputational damage a bank can suffer if the bank is publicly linked to a client their stakeholders would view as negative. Companies in the adult film industry and arms manufacturing have been debanked for primarily reputational reasons. Clearly industries with criminal potential carry an element of reputational threat too; moreover, debanking decisions are subjective, reflecting a qualitative risk. Bank regulators, until 2025, considered reputation risk management as part of their assessment of banks. However, many politicians have argued banks have been debanking organizations for political and legal reasons. In 2025 an executive order in the United States ended the use of reputation risk assessments by federal regulators to make it easier for organizations to file complaints about debanking (Knight et al., 2025). Essentially, debanking decisions themselves became a risk in the United States in 2025. Managers understand reputational risks exist (known) but have a difficult time understanding these risks (unknown).

Enterprise Risk Management

Understanding risk is critical to crisis management and facilitates resilience. Enterprise risk management (ERM), because of its comprehensive view of risk, is a useful framework for crisis management. ERM is a form of business strategy based upon identifying, assessing, and preparing for risks faced by managers that can interfere with the organization's objectives and operations. ERM is a comprehensive risk management approach for organizations designed to cover all risks, including physical (disasters) and symbolic (reputation attacks) (Banerjee, 2016; D'Arcy & Brogan, 2001). It is the integrated aspect of ERM that makes it ideal for crisis management. Multiple units within organizations monitor and manage risk. ERM recognizes there are a variety of risks within an organization but realizes the need to consider organizational risks holistically and not as separate entities. Technology risk is a good way to illustrate ERM. Initially, organizations separated the technology risks (those related to technology) from business risks. The IT department managed the technology risk while the risk management department handled the businesses risk. But when your business operations, perhaps even sales, depends heavily on technology, a technology risk is a business risk. Through an ERM perspective, all risks are treated in a comprehensive and integrated fashion. However, organizations do categorize risks into different types to organize the risk information more effectively. Even the real-time information (information received within minutes of it appearing) collected by organizations tends to be siloed. A Forrester (2021) study found 68% of organizations siloed their real-time information. These risk silos carry over into crisis management. Only 23% of executives felt their crisis management functions were integrated well (PwC, 2021). Integrating risk through ERM should facilitate integration of crisis management as well.

The interrelated nature of risks is a key element of ERM's holistic approach. Risks might be identified and assessed separately, but most risks are related to other risks. Risks can be interrelated by interconnection, overlap, or cascading. Interconnected risks indicate how one risk influences the likelihood, impact, and ways to manage other risks because they coexist in a system. For instance, a cybersecurity breach prompts regulatory attention, which affects reputational and financial assets. Overlapping risks share common drivers, sources, or consequences. An example is the way climate change and supply chain risks overlap when extreme weather events disrupt logistics and production. Cascading risks are connected in a sequential fashion with one risk being realized causing another risk to be realized. Consider how disasters, such as extreme weather events, can create public health crises or how a crisis for a supplier in a company's supply chain can result in delayed production and an inability to fulfill contracts.

The typical risk categories in business organizations are strategic, financial, operational, legal, technology, and reputation. Keep in mind these six categories are interrelated and do overlap with one another but provide a way to start thinking about the variety of risks faced by organizations. Strategic risks involve disruptions to the business plan that make strategy less effective and goals more difficult to achieve. New competitors or technological shifts can create strategic risks. Financial risks relate to how money flows in and out of the organization and sudden financial loss. Economic uncertainties or volatile markets are financial risks. Operational risks are internal risks derived from your business and include your operations and employees. A computer system going down or an employee mistake triggering a chemical release are examples of operational risk. Reputational risks occur when the organization's reputation suffers in some way due to actions or lack of action by an organization.

Legal risks include contract risk, policy risk, liability risk, and compliance risk. Contract risks include breach, inadequate enforcement, and improperly structuring a contract. A supplier causing an operational disruption by not delivering goods on time or litigation resulting from unclear contract terms are examples of contract risks. Contract risks can result in damages and legal costs. Policy risks refer to changes in governmental regulation, policy, or laws that negatively affect an organization's operations. Regulatory changes increasing compliance costs is an example of a policy risk. Liability risks involve an organization being held legally responsible for causing harm to others. Products harming customers, discrimination against employees, and negligence are examples of liability risks. Product recalls due to a product presenting a danger to customers are a highly visible example of liability risks. Liability risks are costly, involving damage awards, settlements, class action lawsuits, and insurance premium hikes. Policy changes can create uncertainty for organizations. (The section on issues management will expand upon this risk.) Compliance involves meeting all required legal and regulatory requirements. Failing to follow proper emission standards at a facility or not meeting the requirement for the Americans with Disabilities Act (ADA) would be compliance risks. Compliance risks can involve a failure to comply with laws, regulations, or internal policies. They can result in financial loss, regulatory or legal sanctions, or reputational loss. Compliance risks can result in fines, operational shutdowns, and license revocation.

In the United States, publicly held companies are required to detail their risk factors in their annual 10-K filings, documents created to provide financial performance data for interested stakeholders. The 10-K reports provide some insights into how companies discuss risk. Below are samples of how some companies have described various risks in their 10-K reports.

> Home Depot, 2024 10-K
> Our customers expect a high level of customer service and product knowledge from our associates. To meet the needs and expectations of our customers, we must attract, develop and retain a large number of highly qualified associates and maintain a productive relationship with those associates. (Home Depot, 2025, p. 13)
>
> McDonald's 2024 10-K
> Our regulatory and legal environment worldwide exposes us to complex compliance, litigation and similar risks that could affect our operations and results in material

ways. Many of our markets are subject to increasing, conflicting and highly prescriptive regulations involving, among other matters, restaurant operations, product packaging, marketing, use of information technology systems, the nutritional and allergen content and safety of our food and other products, labeling and other disclosure practices. Compliance efforts with those regulations may be affected by ordinary variations in food preparation among our own restaurants and the need to rely on the accuracy and completeness of information from third-party suppliers. (McDonald's, 2025a, p. 31)

PepsiCo 2024 10-K

The deadly conflict in Ukraine and related sanctions have continued to result in worldwide geopolitical and macroeconomic uncertainty. The conflict has resulted and could continue to result in volatile commodity markets, supply chain disruptions, increased risk of cyber incidents or other disruptions to our information systems, reputational risk, heightened risks to employee safety, business disruptions (including labor shortages), significant volatility of the Russian ruble, limitations on access to credit markets and other corporate banking services, including working capital facilities, reduced availability and increased costs for transportation, energy, packaging and raw materials and other input costs, environmental, health and safety risks related to securing and maintaining facilities, additional sanctions, export controls and other legislation or regulations (including restrictions on the transfer of funds to and from Russia). (PepsiCo, 2025, pp. 11–12)

Technology risks involve the operations of the organization's technological infrastructure and tend to emphasize cybersecurity. Power outages and data breaches are two common examples of technology risks. Cybersecurity has come to dominate the discussion of technology risks. Box 2.2 examines the growing cybersecurity risk concerns organizations must face. Risk management represents attempts to reduce the vulnerabilities faced by an organization (Smallwood, 1995). Vulnerabilities are weaknesses that could develop into crises. Basically, vulnerabilities are risks. Like crises, not all risks can be avoided or completely eliminated. Hence, risk management involves a number of strategies that vary in their crisis mitigation potential. Risk assessment is the starting point for risk management efforts.

Box 2.2 Cybersecurity Risks

In October 2011, publicly held companies in the United States were encouraged to voluntarily disclose cybersecurity risk in their 10-K reports. Suggested topics to cover included the impact and cost on business activities, the consequences of undetected events, and the impact and significance of incidents. Companies quickly began to include cybersecurity and data privacy into their 10-K reports. Below is part of the cybersecurity risk disclosure from Merck, a pharmaceutical company, in 2024:

The Company's information security group monitors the Company's information systems to prevent, detect, mitigate, and remediate cybersecurity incidents. The Company uses tools and techniques to continually assess and monitor, manage and mitigate cybersecurity threats to its IT systems in a manner consistent with industry practice. The Company engages with key vendors, industry participants, and intelligence and law enforcement communities as part of its continuing efforts to obtain current threat intelligence, collaborate on security enhancements, and evaluate and improve the effectiveness of its information security program. As part of this program, the Company conducts periodic tabletop exercises to assess its cybersecurity incident response processes. The Company also maintains vendor management diligence and oversight processes to identify and monitor potential risks from cybersecurity threats attendant to its use of third-party service providers. Additionally, the Company monitors cybersecurity threat intelligence received from key third-party service providers associated with the Company.

In the event of a cybersecurity incident, the Company has a process in place whereby members of the security group will alert the CISO and the CISO will alert the appropriate levels of management, including an incident assessment team, as well as the legal and finance departments so that the materiality of any such event can be assessed in furtherance of fulfilling any reporting requirements. If warranted, senior management will notify the Audit Committee or the full Board, as appropriate.

The Company has been and continues to be the target of cyber-attacks and network disruptions. To date, the risks posed by such cybersecurity threats have not materially affected the Company and its business strategy, results of operations and financial condition, and as of the date of this report, the Company is not aware of any material risks from cybersecurity threats that are reasonably likely to do so, but there can be no assurance that the Company will not be materially affected by such risks in the future. For further information, see Item 1A. Risk Factors—The Company is increasingly dependent on sophisticated software applications and computing infrastructure. The Company continues to be a target of cyber-attacks that could lead to a disruption of its worldwide operations, including manufacturing, research and sales operations. (Merck, 2025, p. 40)

A more recent development in cybersecurity risks has been misinformation and disinformation (Tuttle, 2021). Misinformation tends to be unintentional while disinformation is intentional. Inaccurate and harmful information are the keys to misinformation and disinformation. The information can harm the organization and perhaps even stakeholders. Deepfake is a rising concern for organizational risk managers (Tuttle, 2021).

The discussion of technology risks would be incomplete without considering artificial intelligence (AI) risks. Since 2023, we have seen an increase in U.S. companies reporting AI risks in their 10-K reports (Mirbagheri, 2025). In 2024, the U.S. government noted a concern about AI washing, particularly in the financial sector. AI washing is when an organization overstates its use of AI and the capabilities of their AI. For example, Delphi Inc. was fined for claiming it was using an AI-powered investment platform when the platform lacked significant AI algorithms. Furthermore, companies are identifying the risks AI poses to their operations, such as enhanced cyberattacks and misinformation/disinformation generation (Peterman et al., 2024).

Risk assessment attempts to identify risk factors or weaknesses and to assess the probability that a weakness will be exploited or developed into a crisis (Levitt, 1997; Pauchant & Mitroff, 1992). Every organization faces a variety of risk factors. Typically, they include personnel, products, the production process, facilities, competition, regulations, and customers (Barton, 2001). Risk factors exist as a normal part of an organization's operation. The following incidents illustrate their crisis potential: In November of 2022, Andre Bing, an employee at the Walmart in Chesapeake, Virginia, walked into the breakroom and began shooting. Six people were killed and two were injured in the shooting. Bing then shot himself. On August 11, 2025, an explosion occurred at the Clairton Coke Works, a facility owned and operated by U.S. Steel near Pittsburgh, Pennsylvania. Two workers were killed by the blast and 10 were hospitalized. The facility suffered heavy damage. In September 2025 Makita recalled over 62,000 professional cordless grease guns. Five people had received lacerations when holes developed in the grease gun hose. Grease ejected from the hose created a laceration hazard. This is an example of product and customer risk.

Risk assessment is both internal and external. The internal weaknesses identified through risk assessment provide vital information for crisis management scanning. For instance, Occupational Safety and Health Administration records might reveal a pattern of mishandling acids. The crisis team concerned would look for ways to break the pattern, thereby preventing injuries and reducing a crisis-inducing risk factor. Similarly, scanning of the external environment can identify risks that could manifest into crises.

Risk assessment requires (a) the identification of possible risks (potential threats) and categorization of risks and (b) an analysis of each risk. The preceding discussions of risk in this chapter suggest various categories of risk for managers to include in their risk assessments as starting points for identifying risks. Typically, risks are assessed using likelihood (probability) and impact (severity). Likelihood and impact become the dimensions for the risk matrix. Assessment primarily is a qualitative process of a team assessing the likelihood and impact of each risk on some scale (Donovan, 2025). The risk matrix in Table 2.1 is a 5 × 5 matrix meaning the team assesses both likelihood and impact on a scale of 1 to 5 with 1 being the lowest and 5 being the highest score. The risk matrix is a visual tool for mapping the risk assessment. The scores in the matrix allow the team to then prioritize the risks (Kovačević et al., 2019; Vincento, 2024). The highest risks warrant further attention and potential mitigation, the focus of Chapter 3. Because of VUCA (volatility, uncertainty, complexity, and ambiguity), risks change and are not stagnant. Teams must meet regularly to update the crisis matrix because risk assessments do change over time and new risks can emerge. Regularly means at least quarterly; many organizations requiring their risk teams to meet every month.

Table 2.1 ▪ Sample Risk Matrix

	Impact				
Likelihood	**Negligible**	**Minor**	**Moderate**	**Significant**	**Severe**
Very Unlikely	Negligible Risk	Negligible Risk	Low Risk	Moderate Risk	Moderate Risk
Unlikely	Negligible Risk	Low Risk	Low Risk	Moderate Risk	High Risk

(*Continued*)

Table 2.1 ▪ Sample Risk Matrix (*Continued*)

Impact					
Possible	Negligible Risk	Low Risk	Moderate Risk	High Risk	High Risk
Likely	Negligible Risk	Low Risk	Moderate Risk	High Risk	Major Risk
Very Unlikely	Low Risk	Moderate Risk	High Risk	Major Risk	Major Risk

Velocity is a new addition to risk assessments. Velocity is how quickly a risk will affect an organization once it is realized. Velocity is calculated using the same scale applied to likelihood and impact. Velocity can be added to the risk matrix using colors or shapes to indicate high, moderate, or low. For instance, high velocity could be color coded red or use a large red circle, moderate velocity could be yellow or use a medium-sized red circle, and low velocity could be green or a small red circle.

A risk matrix helps managers to determine what risks are important to them. Generative AI can be used as another set of eyes to review the risk matrix and suggest possible revisions by identifying overlooked risks. Managers can then review the suggestions to determine the utility of the advice. The risk matrix then guides efforts to find emerging risks in the external and internal environments. This often requires managers to sift through what is called "big data." *Big data*, a term popularized by Doug Laney, refers to the large volume and variety of data (structured and unstructured) that an enterprise can accumulate quickly and continually. For strategic communication such as crisis communication, big data represents an approach whereby technology is used to analyze large data sets in order to facilitate decision-making. Big data can be used to help enterprises set strategies and execute tactics that facilitate achieving their objectives. In big data the utility comes from how you use the data, not by how much data you have. About 80% of the data that comprise big data are unstructured, meaning they are unorganized (Weiner & Kochhar, 2016). Think of structured data as what you would find in a spreadsheet. Common examples of unstructured data would be social media posts and news stories. Big data transforms raw data into actional information, information that is useful for problem-solving and decision-making. Essentially a big data approach is a form of knowledge management whereby various patterns and meanings are found in the data, thereby creating actional information.

Tackling big data is the forte of AI. Classification AI can categorize the risk-related data and place them within the boxes identified in a risk matrix. Anomaly detection AI can quickly spot atypical events indicative of an emerging risk while agentic AI can be used to automate the risk identification and classification process. We must remember that human intelligence (HI) is needed to check on the process and determine the true salience of possible risks. All final decisions made in the crisis communication process should be provided by humans. The various types of AI are all potential assets for the crisis managers and the crisis teams. The various types of AI can review data and provide potential actionable insights with the information they can generate and advice they can provide. All five types of AI can perform tasks similar to those provided by various crisis team members, tasks such as drafting messages, answering queries, evaluating data, and making recommendations for action. We can think of the types of AI as members of the crisis team, in a way. However, as with all crisis team members, their recommendations for action still need to be vetted and the information they provide must be verified.

Ideally, firms want to use a unified data warehouse approach when applying the various types of AI. Too often, firms have multiple, siloed databases. AI expert Andrew Ng (2018) recommends centralizing data into one or just a few data warehouses. Having all the data in one place makes it easier for AI to find patterns. The centralizing of data is a theme found in risk management and crisis communication. This centralization of data is consistent with the ERM approach that argues all risks should be combined and examined holistically rather than fragmented and analyzed by different units within a firm. This includes combining traditional risks, such as safety, with reputational risks (Banerjee, 2016). Military intelligence argues for an "all sources" approach to intelligence that seeks data from all available sources to assess a situation (Philp & Martin, 2009). Crisis communication has long argued for creating a crisis sensing network that funnels all potential crisis risks to one location for analysis (Coombs, 1999). By reducing the problems created by information overload (Kaufhold et al., 2020), the various types of AI make the utilization of one, centralized risk data warehouse viable and provides a more holistic analysis of risks.

ERM needs to be supported by a strong risk culture and employees being risk curious. A strong risk culture places an emphasis on risk awareness and how it is every employee's job to identify risks and to discuss those risks with others. Such a mindset helps an organization to identify and to mitigate risks (ZenGRC, 2024). Risk-curious employees actively try to find and to discuss risks with managers. Employees are risk sensors because they can be exposed to risk through their daily activities. However, the employees need to be encouraged to be risk curious as part of a strong risk culture. Employees must understand there is an expectation of identifying and reporting risks to management. Managers must discuss risks with their employees to reinforce the value of risks (Zanin et al., 2016). A strong risk culture and a sense of risk curiosity can help to combat the emergence of unknown-knowns. Unknown-knowns can flourish when people choose not to discuss risks or are activity discouraged from reporting risks. Risks can be labeled as negative information, making discussion of risks unpleasant and unlikely within an organization and thereby encouraging unknown-knowns. The *MUM effect* is the term used to describe when people do not share negative information in an organization (Bisel et al., 2012). We will return to the MUM effect and unknown-knowns in Chapter 6. Oddly, only about 7% of companies monitor changes in emerging risks daily while most (43%) execute such checks quarterly (Donovan, 2025). This would suggest a general lack of risk curiosity in most organizations.

Knowledge management is a term used to describe how managers in organizations systematically collect, organize, share, and leverage knowledge. Knowledge refers to data (information) that has been interpreted in some way—given meaning. The primary goals of knowledge management are to facilitate decision-making and improve efficiency (reduce the time it takes to find and access knowledge) (Bloomfire, 2025). The discussion of risk demonstrates how knowledge management is an essential element of crisis management. Crisis managers and the crisis management team are constantly collecting, organizing, sharing, and using that knowledge to inform their decisions and actions.

Box 2.3 Crisis Leadership Competencies

Creativity

Crisis leaders need creativity because crises create new and unique situations. No two crises are exactly alike, which means leaders are required to deal with novel events during a crisis. One aspect of creativity is the ability to create new and useful ideas (James & Wooten, 2010). By combining ideas from issues management, risk management, reputation management, and crisis management, leaders can create unique ideas that can be useful during a crisis. Knowledge from all four areas can be useful during a crisis. Another aspect of creativity that is essential in crises is the ability to project the path of a crisis warning sign. Conceptual combination is a recognized means of facilitating creativity; different concepts are combined to create an original and more complex concept (Kohn et al., 2011). Issues management, risk management, and reputation management provide different ways to visualize the potential path of a crisis warning sign. These three approaches can be fused through conceptual combination to provide new insights into the projected trajectory of crisis warning signs. The idea of projecting the effect of crisis warning signs is discussed further in Chapter 3. This is one example of how the crisis management team creativity and leadership should encourage and value such creativity.

Chapter Summary

Risk is the foundation for crisis management. This chapter presented different ways to understand and to categorize with a focus on risk. The knowns and unknowns framework for risk helps managers to appreciate the value and complications with qualitative risks and to identify potential blind spots in their approaches to risk. Issues management and reputational risks are unique forms of risk that required further explication. Enterprise risk management (ERM) reinforces the need to view risk holistically because of the interrelatedness of risk. ERM seeks to place all organizational risks into one system. This is useful in crisis management because crisis risks can be distributed throughout an organization and found in various departments. Managers freely acknowledge these departments frequently fail to share risk information with one another. To be effective, crisis managers need to see across all organizational areas to find possible crisis risks. The next two chapters explore how crisis managers attempt to identify and to mitigate risks.

Discussion Questions

1. Why should reputation and issues management be considered special forms of risk?

2. How do you think perception gaps form? Does their formation help to inform how you would correct a perception gap?
3. What does it mean to say a risk can develop into a crisis?
4. What makes issues management unique as a risk?
5. Would you argue for an organization to create a separate department to manage reputational risks? Why or why not?
6. What makes reputational risk so difficult to manage?
7. Why is ERM valuable to crisis management?
8. How do paracrises contribute to risk evaluations?
9. What are the various ways social media add to organizational risk?
10. When and how can corporate social responsibility (CSR) become a risk?
11. How does the known-unknown framework help us to understand risks?
12. Why are qualitative risks so challenging?
13. Why add velocity to the risk matrix?