CHAPTER

2

Risk as the Foundation for Crisis Management and Crisis Communication

CHAPTER OBJECTIVES

Enterprise Risk Management

- Defend why risk is essential to crisis management.

Risk in the Organizational Context

- Explain how social media has been reshaping organizational risks.

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.

Risk can be defined as "uncertainty about and severity of the consequences (or outcomes) of an activity with respect to something that humans value" (Aven & Renn, 2009, p. 1). 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, 2020). 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) (Ernst & Young, 2020). This chapter begins with the enterprise risk management (ERM) approach as a way to understand how various elements within an organization can contribute to crisis management followed by an explanation of the organizational context for risk. The organizational context for risk includes stakeholders and risk, issues management, and reputational risk. This chapter explores the many facets of risk crisis managers face through the framework of ERM.

ENTERPRISE RISK MANAGEMENT

Risks are the foundation of crisis management and communication because risks are vulnerabilities that could develop into crises. Moreover, risks reflect the duality of threat and opportunity. Every threat has an element of opportunity while each opportunity has an element of threat. Risks pose a threat but can be an opportunity as well if handled skillfully. We see this same duality of threat and opportunity with crises. A crisis does threaten an organization and its stakeholders but is an opportunity for the organization if the crisis is managed skillfully. Risk and crisis are intricately linked to one another. As Heath and Palenchar (2009) noted, a crisis is a "risk manifested" (p. 80). A risk has the potential to do harm while a crisis is inflicting harm. Understanding risk is critical to crisis management and facilitates resilience. 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 business 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 typical risk categories in business organizations are strategic, financial, operational, compliance, 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.

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. 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.

Reputational risks occur when the organization's reputation suffers in some way due to actions or lack of action by an organization. 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. A 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 (2021a, 2021b) Global Risk Dialogue white paper centered on reputational/social evaluations risks. The white paper focused on environmental, social, and governance or ESG risks. Environmental risks include climate change, pollution, resource depletion, waste, ecological footprint, and green building. Social risks include working conditions, local communities, supply chains, health and safety, employee engagement, customer relations, and data. Governance risks include executive pay, corruption and bribery, board diversity, director and officer liability, taxes, and cybersecurity. ESG risks are driven by social evaluations because they shape the perceptions of an organization. ESG risks can create "bad news" (negative media coverage or discussions) that can harm an organization (Allianz, 2021a, 2021b). One example is greenwashing. Greenwashing is when an organization makes fraudulent or inflated claims about its proenvironment actions. Exposure of greenwashing used to just create bad press, now it can result in litigation by governments and increased regulation.

Starting in 2005, publicly held companies were required by the Securities and Exchange Commission (SEC) to detail risk factors in their 10-K filings. A 10-K document is created by publicly held companies to provide detailed financial performance data for interested stakeholders. The risk factors section represents one of five major sections in a 10-K report. The risk factors detail all risks a company faces and is usually listed in order of importance with the most important risk being listed first. The risk factors section began to appear in

the 2006 10-K reports of companies. Below are actual descriptions of risks corporations have provided in their 10-K filings that illustrate the six categories of risk:

Strategic Risks

If we pursue strategic acquisitions or divestitures, we may not be able to successfully consummate favorable transactions or successfully integrate acquired businesses.

(Tyson, 2015, p. 11)

Failure to continually innovate and successfully launch new products and maintain our brand image through marketing investment could adversely impact our operating results.

(Tyson, 2015, p. 9)

Financial Risks

Deterioration of economic conditions could negatively impact our business.

Our business may be adversely affected by changes in economic conditions, including inflation, interest rates, access to capital markets, consumer spending rates, energy availability and costs (including fuel surcharges) and the effects of governmental initiatives to manage economic conditions. Any such changes could adversely affect the demand for our products, or the cost and availability of our needed raw materials, cooking ingredients and packaging materials, thereby negatively affecting our financial results.

(Tyson, 2015, p. 12)

If we are unable to anticipate consumer preferences and develop new products, we may not be able to maintain or increase our revenues and profits.

(Nike, 2015. p. 7)

Operational Risks

We depend on the availability of, and good relations with, our employees.

We have approximately 113,000 employees, approximately 36,000 of whom are covered by collective bargaining agreements or are members of labor unions. Our operations depend on the availability and relative costs of labor and maintaining good relations with employees and the labor unions. If we fail to maintain good relations with our employees or with the labor unions, we may experience labor strikes or work stoppages, which could adversely affect our financial results.

(Tyson, 2015, p. 8)

If our internal controls are ineffective, our operating results could be adversely affected.

(Nike, 2015, p. 12)

Compliance Risks

Legal claims, other regulatory enforcement actions, or failure to comply with applicable legal standards or requirements could affect our product sales, reputation and profitability.

We operate in a highly regulated environment with constantly evolving legal and regulatory frameworks.

(Tyson, 2015, p. 11)

Reputational Risks

Failure to maintain our reputation and brand image could negatively impact our business.

Our iconic brands have worldwide recognition, and our success depends on our ability to maintain and enhance our brand image and reputation.

(Nike, 2015, p. 7)

Failure of our contractors or our licensees' contractors to comply with our code of conduct, local laws and other standards could harm our business. Significant or continuing noncompliance with such standards and laws by one or more contractors could harm our reputation or result in a product recall and, as a result, could have an adverse effect on our sales and financial condition.

(Nike, 2015, p. 11)

Technology Risks

Failures or security breaches of our information technology systems could disrupt our operations and negatively impact our business. Information technology is an important part of our business operations and we increasingly rely on information technology systems to manage business data and increase efficiencies in our production and distribution facilities and inventory management processes.

(Tyson, 2015, p. 11)

If the technology-based systems that give our customers the ability to shop with us online do not function effectively, our operating results, as well as our ability to grow our e-commerce business globally, could be materially adversely affected.

(Nike, 2015, p. 11)

Box 2.1 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

BOX 2.1 BRAND SAFETY CRISES

In October of 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 (EY, 2020). Below is part of the cybersecurity risk disclosure from Apple in 2020:

> *There may be losses or unauthorized access to or releases of confidential information, includ-ing personally identifiable informa-tion, that could subject the Company to significant reputational, financial, legal and operational consequences.*
>
> *The Company's business requires it to use and store confidential information including, among other things, personally identifiable information ('PII') with respect to the Company's customers and employees. The Company devotes significant resources to network and data security, including through the use of encryption and other security measures intended to protect its systems and data. But these measures cannot provide absolute security, and losses or unauthorized access to or releases of confidential information occur and could materially adversely affect the Company's reputation, financial condition and operating results.*
>
> *For example, the Company may experience a security breach impacting the Company's information technology systems that compromises the confidentiality, integrity or availability of confidential information.*
>
> (Apple, 2020, p. 12)

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).

crisis mitigation potential. Risk assessment is the starting point for risk management efforts.

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: Very late on an August night in 2012, recent hire Terence S. Tyler entered the Pathmark grocery store in Old Bridge, New Jersey. He then began firing an AK-47 assault rifle, killing two coworkers, 18-year-old Christine Lo Brutto and 24-year-old Bryan Breen, before killing himself. This is an example of personnel risk (Gingras, Dienst, Thompson, & Creag, 2012). In September of 2020, a dust explosion injured two employees at a woodworking company in Stützengrün, Germany. The blast sent four workers to the hospital with burns and caused the evacuation of local homes. This is an example of a production process risk. In October 2020, Pelton recalled about 27,000 bikes with PR70P pedals. Some 120 customers reported the pedals fell off resulting in 12 reported injuries. 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.

Once a risk is identified, decisions are made about risk aversion—the elimination or reduction of a risk. Two factors drive the use of risk-aversion decisions. The first factor is cost. Risk managers use procedures such as risk balancing to compare the costs of the risk (e.g., costs of deaths, injuries, litigation, and property damage) to the costs of risk reduction (e.g., equipment and actual work needed to prevent or reduce the risk). Organizations may take no action when the costs of risk reduction outweigh the costs estimated from the risk. However, ignoring risk can be a more costly move than anticipated. If stakeholders discover their safety was sacrificed for profit, a different and much worse type of crisis erupts. In May 2010, documents were released that shed new light on BP's deadly 2005 Texas City refinery explosion. Lawyer Brent Coon released a two-page BP document that showed the company favored profit over human safety and lives. The memo was a cost–benefit analysis of trailers to be used at Texas City. Most of the 15 fatalities from the explosion were workers in these trailers. The memo showed a value of $10 million for a human life in the calculation to determine which type of trailer to buy. BP concluded that blast-resistant trailers were too expensive, costing 10 times more than the less protective trailers BP did buy for Texas City. The most disturbing aspect of the memo was that it used the analogy of the three little pigs, with the pigs being the workers and an accident being the big bad wolf. The final conclusion from the memo was that human life had a price and BP was not willing to overpay to protect workers—finance trumped human safety (Outzen, 2010).

When managers choose to engage in risk aversion, risk management becomes crisis mitigation. Actions are taken to completely eliminate the risk or to reduce it to as low a level as reasonably possible (Levitt, 1997). The use of dangerous chemicals in a manufacturing process illustrates this point. Using inherently safer practices is an approach to designing safer chemical plants, storage facilities, and chemical processes. Three common risk-reduction strategies resulting in inherently safer practices are to (1) reduce the amount of hazardous material on site, (2) substitute a less hazardous substance, and (3) use a less hazardous process or storage condition. If less hazardous materials are on site,

the effect of a crisis is reduced: The Chevron Richmond Refinery reduced the amount of anhydrous ammonia it stored on site and moved the storage facilities farther from the nearby residential area. If a nontoxic or less hazardous chemical can be substituted for a hazardous chemical, a risk can be eliminated or reduced: The Mt. View Sanitary District, a wastewater treatment facility, replaced three hazardous chemicals (chlorine, sulfur dioxide, and ammonia) with an ultraviolet light system to disinfect wastewater. Changes in the chemical process used or the state in which a chemical is stored can reduce a hazard: Acrylate producers have switched from manufacturing with the Reppe process to the safer propylene oxidation process, and Dow Chemical switched from using liquid chlorine to the less hazardous gaseous form.

Using inherently safer practices is one among a variety of approaches for eliminating or reducing risk. Another common effort is training, and topics related to risk aversion can range from chemical safety to email use. The exact action taken by an organization to reduce a risk varies according to the actual risk (Lerbinger, 1997). For instance, many companies face computer rather than chemical risks. Antivirus software, firewalls, and employee Internet use policies are ways to prevent risks. Consider the threat of viruses, such as the one known as Melissa that could damage an organization's computer systems and databases. Cognos Corporation, a software developer, knew that the Melissa virus contained a file that was over 25K in size. The company set a 25K limit on incoming messages to keep Melissa out. Managers acted quickly; within one hour of identifying the risk, a policy was created and relayed to employees along with a rationale for the new policy (Meserve, 1999). The basic process involves determining whether the risk aversion is possible and then implementing the risk aversion program.

When a risk becomes manifest, a crisis can occur. Failure to reduce the risks associated with the start-up of the isomerization unit at Texas City manifested itself in an explosion that killed 15 workers and injured over 170 others at the BP facility. Crises often create new risks. The oil from the Deepwater Horizon oil platform explosion in 2010 triggered multiple crises for those in the tourism and fishing industries in the Gulf of Mexico and beyond. Moreover, crisis communication may require the discussion of risk and the need to engage in risk communication, "a communication infrastructure, transactional communication process among individuals and organizations regarding the character, cause, degree, significance, uncertainty, control, and overall perception of risk" (Palenchar, 2005, p. 752). Risk communication is essentially a dialogue between the organization creating the risk and the stakeholders who are asked to bear the risk. Organizations explain what the risks are and what can be done to protect people from the risk, while stakeholders explain their concerns about and perceptions of the risk. Risk communication is a topic we will explore throughout the book.

RISK IN THE ORGANIZATIONAL CONTEXT

ERM involves risk management within organizations. Therefore, it is important to consider risk within the organizational context. What this means is we need to appreciate the unique forms of risk faced by organizations. The organizational context of risk can be explained by understanding the connections between stakeholders and risk, issues management as risk management, and the importance of reputational risks.

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 ERM and how to understand organizational risks. The discussion of stakeholders begins by clarifying their relationship to risk and 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 also 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 that create conflicts between themselves and the organization. Organizational success is predicated on maintaining an effective balance in these relationships (Donaldson & Preston, 1995; Rowley, 1997; Savage, Nix, Whitehead, & Blair, 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).

In 2004, Kryptonite announced it would recall some of its popular and high-priced bicycle locks. The problem was that many locks could be picked using just the outside casing of a Bic pen. The impetus for the recall was a complaint from a group of angry bikers taking their case to the Internet via discussion group postings and blogs. Some people even posted videos showing how to pick the lock, to prove the claim was true. The bikers were angry that their very expensive bikes were being stolen or were at risk from the faulty locks. It took Kryptonite a week to respond to customer concerns, a long time in the Internet world (Wagstaff, 2006). Primary stakeholders are powerful because it is difficult and often impossible to replace the contributions they provide to the organization (Mitchell, Agle, & Wood, 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.

In December 2013, the *Los Angeles Times* ran a story detailing how Wells Fargo employees were being pressured to sell services and that the pressure was causing unethical behaviors. The unethical behavior included opening accounts customers did not need and ordering credit cards for customers without their consent. In September 2016, the Consumer Financial Protection Bureau announced Wells Fargo employees had opened over two million unauthorized customer accounts. Shortly thereafter, then CEO John Stumpf admitted the problem. He resigned the following month. In March 2017, Wells Fargo settled a class action lawsuit over the accounts for $110 million, and new CEO Tim Sloan announced reforms to prevent such abuses in the future. The final internal report conducted by Wells Fargo indicates a total of over 3.5 million fake accounts had been created (Peltz, 2018). The Wells Fargo account fraud crisis was precipitated by a story in the news media that then spread to other stakeholders.

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. Adidas has filed multiple lawsuits against Forever 21 for violating its three stripe trademark. This includes lawsuits in 2015, 2017, and another legal battle in 2019. Adidas has forced Forever 21 to not use "their" tree stripes on merchandise. Adidas argued that people will be confused and buy the merchandise because they think it is adidas. Adidas has repeatedly forced Forever 21 from using the three stripes (Timeline, 2017). The legal actions by adidas (a competitor) did affect the behavior of Forever 21.

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 (Chen, 2019). Organizations, like people, can do things intended to be good but end up embarrassing them—commit 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 examine of a challenge paracrisis is when some stakeholders claim an organization is sourcing raw materials in an irresponsible manner or engage 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 2.2 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).

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

BOX 2.2 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 and the 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 because the situation is more of a paracrisis (guilt by association) because it is about managing a risk rather than an operational crisis. Still the brand safety paracrisis is a threat that crisis managers must consider.

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 account and posted information about employees engaging in illegal activities.

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 stakeholders are the ones to 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.

Issues Management

An issue is "a trend or condition … that, if continued, would have a significant effect on how a company is operated" (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 we will consider the expansion of issues management into social issues.

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.

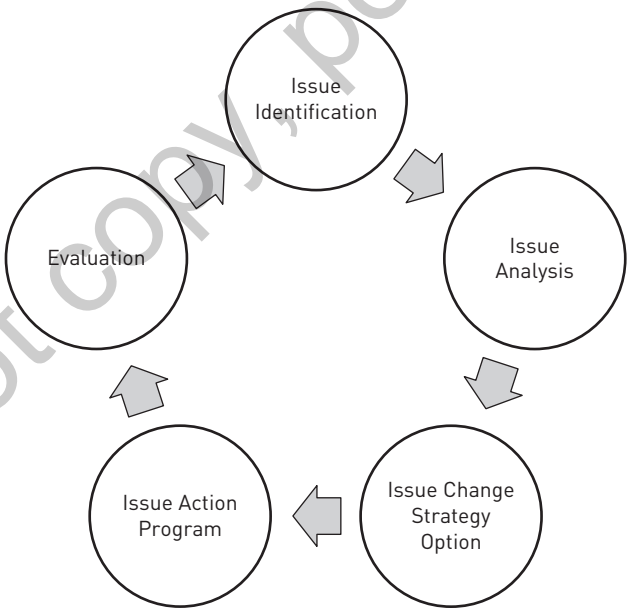
The Jones and Chase (1979) model (issue identification, analysis, change strategy option, action program, and evaluation) is the classic model familiar to most people involved in issues management. The action step centers on communicating the organization's position on the issue to stakeholders involved 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 protrucking 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 protrucking 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 (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

FIGURE 2.1 Jones and Chase Issues Management Model



Source: Based on the Jones and Chase Issues Management Model.

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 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. When three students were killed in the 2000 Seton Hall dormitory fire, new legislation was passed in New Jersey requiring all dormitories to have sprinkler systems. Ineffective management of the Exxon Valdez crisis helped to block oil exploration in the Arctic National Wildlife Refuge for decades. The laxative market offers an example of how issues management can both avert and create a crisis. Until the 1990s, the main ingredient in the two leading laxatives, Correctol and ex-lax, was phenolphthalein. In the early 1990s, the FDA began investigating a link between phenolphthalein and cancer. In 1995, the preliminary study with rats indicated that phenolphthalein could be a carcinogen. The FDA now thought about banning phenolphthalein. Novartis, the manufacturer of ex-lax, did not see a problem and defended the use of phenolphthalein. Schering-Plough, the maker of Correctol, decided to switch from phenolphthalein to bisacodyl and supported the FDA move to ban phenolphthalein.

Additional evidence was collected by the FDA that supported the phenolphthalein–cancer link. In April 1997, the FDA went public with its cancer concern over phenolphthalein. Schering-Plough supported the decision and informed customers that it had removed phenolphthalein from Correctol over a year earlier, while ex-lax still used it. Novartis kept fighting the phenolphthalein ban issue. The company advocated a public education campaign to curb laxative abuse. The idea was that proper, limited use would not place people at risk, that only those who abuse laxatives were at risk for cancer. In August 1997, the FDA proposed a ban on phenolphthalein. At that time, Novartis recalled ex-lax and introduced a new formula shortly thereafter. However, Correctol had already established its competitive advantage by demonstrating greater concern for customers because Schering-Plough had acted much faster to protect customers from the phenolphthalein threat (McGinley, 1997). This case shows how an issue can become a risk for an organization. If the risk becomes manifest, as it did for Novartis, the issue will create a crisis. Issues management offers established methods for managing this unique form of risk.

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. The emergence of social issues management reflects the growing sociopolitical context that expects companies to take action of social issues (Arenstein, 2020; Komiya, 2020). We saw these expectations most recently in 2020 and the Black Lives Matter (BLM) movement which pressured many corporations into policy changes related to hiring, awarding contracts, and even changing logos and names for products.

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 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, Holladay, & White, 2021).

Reputational Risk

A reputation is an evaluation stakeholders make about an organization. Hence, we can talk about favorable and unfavorable reputations. As noted earlier, reputation is one form of social evaluation that generates social approval assets and liabilities. 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 do 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 noted earlier 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 ERM 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, Friedrich, Wiemann, and Wiemann (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 (Smith, 2012).

Crisis managers must now consider CSR activities as a form of crisis risk. CSR activities generate two 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, 2015). 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, 2015). For instance, H&M does engage 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.

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.

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. All 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. Issues management, risk management, and reputation management provide different ways to visualize the potential path of a crisis warning sign. Combining the proactive management functions should 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.

CHAPTER SUMMARY

Risk is the foundation for crisis management, making ERM an ideal starting point for our discussion of crisis management and crisis communication. ERM seeks to place all organizational risks into one system. This is useful in crisis management because crisis risks can be distributed throughout an organizational and found in various departments. Managers freely acknowledge these department frequently fail to share risk information with one another. Issues management and reputational risks are unique forms of risk that required further explication. To be effective, crisis managers need to see across all the 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 its 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 add to risk evaluations?
9. What are the various ways social media add to organizational risk?
10. When and how can CSR become a risk?