3

THE CRISIS MITIGATION PROCESS

Building Crisis Resistant Organizations

The best way to manage a crisis is to prevent a crisis. If crisis managers can locate and resolve a risk before it becomes a crisis, stakeholders and the organization are spared any harm. Crisis expert Tony Jaques likes to use the term "crisis proofing" to refer to actions to protect an organization from risks and crisis damage. However, he admits that it is impossible to make an organization completely immune from all crises (Jaques, 2016). A more accurate term would be to make an organization "crisis resistant." Be very skeptical of any consultants who claim they can make your organization immune from crises. Many products have tamper resistant packaging because the original tamper proof was misleading. We see the same problem with crisis prevention—the term is too strong. That is why I am using the term *mitigation*. Mitigation means to lessen the effects of something. Many crises cannot be prevented; crisis managers can hope only to mitigate the occurrence or the effects of a crisis. The term *prevention* can mean a hindrance in addition to keeping something from occurring; but this chapter uses the term *mitigation* to avoid confusion. To create a crisis resistant organization, crisis managers take actions designed to eliminate a crisis threat or to reduce the likelihood of the threat manifesting into a crisis. From an enterprise risk management perspective, all areas of the organization that address risk must be combined to create a holistic approach to crisis mitigation, including issues management, risk management, and reputation management.

Crisis mitigation is about finding and responding to red flags. The term *red flag* has been used to denote a warning sign for hundreds of years. Crisis managers must locate and respond to red flags if there is any chance of mitigating a crisis risk. Boyd's OODA Loop is perfect for crisis mitigation because of the emphasis on finding and responding to stimuli in the environment. At its core, crisis mitigation is about responding to stimuli. Therefore, Boyd's OODA Loop is used to organize the explanation of the crisis mitigation process.

OBSERVE: FINDING RED FLAGS

Observing involves understanding where to look for crisis risks and how to collect the information. Where to find the risks is the most challenging aspect of observing. Sources of risk will be both external and internal to the organization, demanding the review of a wide array of sources. Environmental scanning is a tool that is popular in issues management and that focuses on external risks (Gonzalez-Herrero & Pratt, 1996; Heath, 1997; Heath & Nelson, 1986; Pauchant & Mitroff, 1992). Basically, environmental scanning means watching and listening to the environment for changes, trends, events, and emerging social, political, or health issues. The information is used to guide organizational decision-making to plot future actions (Lauzen, 1995). Crisis managers must consider the sources involved in external scanning that would be helpful in locating warning signs. The exact mix of sources to scan will vary from organization to organization. However, we can identify some broad categories of external sources that should be scanned.

Media are an essential element of the external environment for crisis managers. Media include the traditional news media and rapidly expanding digital channels and platforms found online. The news media include leading or elite newspapers (e.g., *New York Times, Wall Street Journal, Washington Post*), news and business magazines (e.g., *Time, Newsweek, Fortune*), and television news programs including TV news magazines (e.g., *60 Minutes*, *20/20*). Of special interest is information about crises in similar organizations. Case studies of similar organizations in crisis are a valuable resource for crisis managers, allowing crisis teams to learn from someone else's crisis rather than their own (Pauchant & Mitroff, 1992).

Other useful media sources (both traditional and digital formats) include trade journals, relevant medical or scientific journals and websites, blogs, newsletters, and public opinion surveys. The trade outlets are likely to carry stories about crises suffered by similar organizations. The trade journals, other publications, blogs, and websites provide information about issues the industry is facing as well as industry-specific complaints. All can help to identify possible crises for individual organizations within that industry. Medical or scientific journals and websites may contain studies that could affect how people view an industry. The dangers of cholesterol and concerns over the link between cell phone use and automobile accidents are examples of pertinent study topics. The public's first exposure to these two health concerns was through medical and scientific publications, not the news media.

Digital newsletters include reports published by special interest groups, foundations, and government agencies. Each can indicate potential threats to an organization. Special interest media inform organizations about the concerns of activist stakeholders and indicate if anger is being focused on their industry or their specific organization. Activists frequently use websites and various social media platforms to present their ideas and concerns. Foundations can identify emerging issues. Government publications and online portals offer insights into possible regulatory or legal changes and identify emerging issues. For example, the *Federal Register* has information about potential regulatory changes, the *Congressional Record* and *Congressional Quarterly Weekly Report* provide information about new legislation, and the *Congressional Quarterly Researcher* provides information about salient issues in U.S. society. Public opinion surveys can indicate changes in attitudes, lifestyles, and values (Heath, 1997).

Individuals are another source of environmental information. Crisis managers should focus on three broad categories: public opinion experts, activists, and the organization's own stakeholders. Because people are increasingly digital naturals, crisis managers must be examining the digital communication channels and platforms. Public opinion experts, like the published data, provide insights into public attitudes, lifestyles, and values. Crisis managers should know who the influential bloggers are in their industry and follow what they are saying.

Any stakeholder can tell the organization how they feel about issues and organizational actions (Heath & Nelson, 1986). The various digital channels and platforms, including social media, make it very easy for stakeholders to express themselves and provide an opportunity for crisis managers to listen to those voices. The digital channels and platforms include but are not limited to discussion groups, message boards and forums, web pages, dedicated complaint sites, blogs, microblogs, content-sharing sites, aggregators, and social bookmarking and social networking sites. The challenge for crisis managers is knowing where to look in the digital world to find crisis risks.

All a person needs is Internet access and the ability to use a keyboard to utilize digital channels and platforms. Admittedly, most social media is of little interest to anyone. However, it is a potentially powerful form of word-of-mouth information distribution (Laczniak, DeCarlo, & Ramaswami, 2001). Word-of-mouth is recognized as a serious force that can shape consumer decisions; hence, it should not be ignored (Blackshaw & Nazzaro, 2004). Consider how concerned organizational leadership has been with critical digital content about their organizations since digital channels and platforms became popular (Holtz, 1999). An example is useful here. In 2018, H&M ran on online advertisement for a child's hoodie in the United Kingdom. Some people, including NBA great LeBron James, thought the saying on the hoodie was racist and took to Twitter to expose H&M's racism. The Tweets were liked and retweeted by thousands of people (Nembhart, 2018). No organization wants to be the "racist" organization; hence, H&M took down the advertisement and apologized for the unintentionally racist content saying, "We have got this wrong and we agree that, even if unintentional, passive or casual racism needs to be eradicated wherever it exists" (H&M Group, 2018, para 1). H&M went on to create a new position of diversity leader to help them be more racially sensitive in the future (H&M Group, 2018).

Social media platforms such as Twitter can be a very effective way to listen to stakeholders. Again, most social media posts are irrelevant to an organization, so crisis managers must carefully identify the social media content and other digital content that is most relevant to their concerns or hire a consulting firm to monitor for them. There is a growing legion of companies that can help organizations monitor social media for warning signs. Among the more prominent media monitoring and social media analytics companies are Critical Mention, Meltwater, Cision, Zignal Labs, Burreles Luce, Sysmos, and Hootsuite. Most large public relations agencies such as Edelman and Golin offer social media services. Organizations may choose to develop their own media monitoring system. Examples of organizations with their own media monitoring systems include the Gatorade Mission Control, the Dell Social Media Listening Command Center, and Cisco Social Media Listening Center.

Digital channels and platforms should be viewed as more than a source of risk for an organization; they also can be used to anticipate and respond to potential problems.

An organization concerned with human rights, for example, can peruse a variety of human rights–oriented websites and blogs or follow human rights organizations on Twitter to get a feel for stakeholder sentiments and the development of human rights issues. These insights can guide actions designed to prevent possible crises. The digital channels and platforms help crisis managers to anticipate and possibly avoid emerging problems. The primary use of these centers is customer relations (Ben-Zur, 2011), but the data helps to identify crisis risks. Managers should work with existing organizational resources to develop an organization's crisis-sensing capabilities to avoid duplicating efforts and wasting resources. The social media monitoring centers can be created by the organization itself or in collaboration with a social media monitoring company (Swallow, 2010).

As measurement expert Katie Delayne Paine (2011) notes, "Monitoring mainstream media is not enough" (p. 165). The digital natural population continues to grow, making it an increasingly important environmental information resource. The digital channels and platforms serve as a dual information source: They can be used to access information also found in print or broadcast form, and they can be used to collect information unique to social media. Whether using a social media monitoring service or developing their own social media monitoring center, crisis managers need to know the term *dashboard*. Paine (2011) defines a dashboard as "a technique for simplifying data reporting by displaying a small number of important summary measures together in one location" (p. 234). The term should make you think about a car. The car's dashboard holds the critical data for a driver, including speed, engine temperature, tire pressure, and oil level. A dashboard can be a visual representation of the data generated by the analysis of social media messages. Like drivers, crisis managers can see all the critical information they need on a properly designed dashboard.

Activists represent organized stakeholders seeking to make specific changes in society. Often those changes involve reforming corporate practices the activists view as irresponsible. Consider how activists exposed the use of sweatshops in the apparel industry, resulting in sweeping changes by corporations in that industry. Crisis managers should seek information about what activists are doing relative to their industry. Activist groups have strong digital presences making it relatively easy to monitor what social concerns and issues are being pursued by various activist groups.

The problem with the digital world is that it generates too much information, the vast majority of which is irrelevant to an organization because no one else is paying attention to it. That is why influencers are important to monitor. Influencers might be bloggers, journalists, or social celebrities with large followings. When influencers post, the message has the potential to be distributed to a large number of followers. Be mindful that the nature of the influencers shapes the nature of the stakeholders listening to them. The composition of the followership of a social celebrity will be different from that of a prominent blogger. Crisis managers need to determine which followers are more important to their organization.

Internal

Crisis managers must scan for internal crisis risk too. Risk management emphasizes sources that have more of an internal focus and should be of interest to crisis managers. Total quality management systematically assesses the manufacturing process in order to improve quality. Part of that process is to locate sources of defects (Milas, 1996), which

can trigger the need for recalls (Mitroff, 1994). Environmental crisis exposure includes pollution abatement actions and threats to the environment posed by an organization. Polluting can lead to accidents, lawsuits, protests, or regulatory fines. Legal compliance audits make sure an organization is complying with all federal, state, and local laws and regulations. Failure to comply can result in lawsuits or fines. Financial audits review the financial health of the organization, which can indicate financially oriented crises, such as a shareholder rebellion. Employees and the organizational culture itself should be monitored for risk. In early 2018, female employees at Nike conducted their own survey about gender discrimination and sexual harassment. The data indicated Nike had a workplace that was demeaning to women and actively blocked the career development of women (Creswell, Draper, & Abram, 2018). When the survey and the results made it to CEO Mark Parker, actions were taken to manage the risk. Six male executives were removed from their positions and policy changes were made to compensation and training (Draper & Creswell, 2018). It is important that the risk from personnel and the organizational culture not be overlooked.

Traditional insurance coverage indicates risks worth insuring against. Insurance risks include liability exposure, criminal exposure, and worker compensation exposure. All three areas can produce lawsuits and extremely negative publicity. Natural disaster exposure identifies what Mother Nature might do to the organization. An organization's managers must know if facilities are at risk of crises caused by floods, earthquakes, or volcanoes—natural actions typically not covered by insurance.

Safety, maintenance, and accident records reveal minor problems that could become crises. These records should be examined for patterns. Organizations have what are called near misses—something bad that almost happened. A series of near misses runs the risk of escalating into a major crisis. If there are a number of near misses—say, small hand injuries with a piece of equipment—it is possible that a major injury, such as an amputation or death, could also occur. Action should be taken in the prevention phase to break the pattern of minor accidents. Similarly, a history of the same safety violation indicates that a major accident and injury could occur. Obviously, safety precautions are designed to prevent accidents and injuries. Unheeded, the workplace becomes unsafe and ripe for these troubling and preventable events (Komaki, Heinzmann, & Lawson, 1980).

Employee use of digital channels, digital platforms, and email also are sources of risk. Misuse of these online communication tools can result in information leaks, computer viruses or worms, discrimination and harassment lawsuits, or reduced bandwidth capacity. Concerns over online risks have led most companies to create Internet and email use policies and to use software designed to monitor employee online behavior. Online use policies lack any real meaning if the organization cannot effectively determine whether their policies are being violated. The monitoring software can block access to inappropriate websites, review all emails for inappropriate language, or record and evaluate all employee web activity in terms of business-related and non-business-related site visits. Organizations assume unnecessary risk if they do not have and enforce employee digital channel and email use policies.

Product-tampering monitoring examines the manufacturing process and packaging for susceptibility to product tampering. Product tampering leads to recalls and lawsuits. Behavior profiling identifies the characteristics of potentially dangerous employees, typically those who may become violent. Violent employees can trigger workplace

violence crises. Ethical climate surveys assess the organization for temptations and cultural blinders to problems. Such blinders are located by examining management attitudes and values about important concerns, such as sexual harassment. A weak ethical climate can encourage organizational misdeeds, such as check fraud, sexual harassment, or racial discrimination (Mitroff & McWinney, 1987; Soper, 1995).

Organizational climates actually can facilitate the creation of crises. Let us return to the story about Wells Fargo creating fraudulent accounts for customers mentioned in Chapter 2. The corporate culture was pressuring employees to open new accounts. The need to conform to this pressure was stronger than the ethical concerns of creating accounts customers did not need or did not authorize. It could be said Wells Fargo had a weak ethical climate coupled with a reward system that favored the aggressive creation of new customer accounts at any cost (Maxfield, 2017). Wells Fargo's own climate worked to facilitate rather than to preclude a serious crisis. We could say Wells Fargo was ethically challenged. A similar fate can befall any company that fails to monitor and correct its own ethical climate and aspects of its culture that can promote rather than retard crises.

The sources for reputation monitoring are not well developed, but Table 3.1 identifies some logical choices, which reflect the importance of stakeholders to reputation management, particularly the investor, customer, activist, and community stakeholders. Shareholder resolutions reflect the values and attitudes of those who own stocks. In 2006, Walmart investors rejected six different social responsibility shareholder resolutions, presumably because the resolutions did not reflect their priorities. Resolutions can reflect social concerns, such as support for the UN Global Compact (a set of 10 environmental and social principles), or financial concerns, such as resolutions preventing the "poison pill" as a takeover defense. Shareholder resolutions provide insight into how the stockholders feel about important issues or the organization itself. Stakeholder complaints and inquires help to detect discontent among customers and to discover rumors. Early identification of discontent means that the organization can act to resolve the problem and make a customer happy, maintaining a positive relationship with this stakeholder (Dozier, 1992). As the Pampers example in Box 3.1 illustrates, digital channels and platforms are ideal for finding and addressing stakeholder expectations that are relevant to reputations.

Profit-making organizations cannot survive without customers, which makes them a critical source for reputation signs. Organizations must identify when their actions place customers at risk and when customers are unhappy with organizational operations or policies. In October 1996, an E. coli outbreak linked to Odwalla juices killed 16-month-old Anna Gimmestad and sickened over 70 other people. Odwalla juice was not pasteurized at that time. Pasteurization kills bacteria, but natural juice makers felt it harmed the product. Odwalla began flash pasteurization after the incident. The company launched a quick recall and covered medical expenses for those who were stricken. In addition, Odwalla was one of the first companies to use the Internet as part of its crisis management. It has been praised for its quick and caring response (Baker, n.d.).

However, from a warning signs detection standpoint, Odwalla was a dismal failure. There were a number of warning signs prior to the October 1996 E. coli tragedy. Dave Stevenson, the head of Odwalla's quality assurance, had recommended using a chlorine rinse to increase the killing of bacteria. Senior executives rejected the idea and kept the far less effective acid-wash method. Even the supplier of the acid wash told Odwalla

BOX 3.1

THE PAMPERS CASE

On May 6, 2010, Pampers, a product of Procter & Gamble, issued a news release with the title *Pampers Calls Rumors Completely False*. Here is an excerpt from the news release that summarizes the situation:

> Jodi Allen, Vice President for Pampers, said, "For a number of weeks, Pampers has been a subject of growing but completely false rumors fueled by social media that its new Dry Max diaper causes rashes and other skin irritations. These rumors are being perpetuated by a small number of parents, some of whom are unhappy that we replaced our older Cruisers and Swaddlers products while others support competitive products and the use of cloth diapers. Some have specifically sought to promote the myth that our product causes "chemical burns." We have comprehensively and thoroughly investigated these and other claims and have found no evidence whatsoever that the reported conditions were in any way caused by materials in our product. Independent physicians, highly respected in the field, have analyzed our data and have confirmed our conclusions." (P&G, 2010, para. 1)

Parents were making online comments that Pampers' new version of its product was harming infants. That is a serious charge for a company trying to sell diapers to parents. Parents do not want to buy a product that will hurt their children. Social media (e.g., blogs, microblogs, social networking sites) were the route for spreading the "rumor." The popular social networking site Facebook is a prime example of social media fanning the rumor. A discussion thread on a Pampers page appeared, claiming that Pampers created severe diaper rash, which even included blistering. The Facebook page had over 10,000 members, many of whom were parents who posted their concerns and experiences on the page. Pampers has its own Facebook page with over 100,000 fans, and even that page had parents posting stories of bad reactions to new Pampers under the discussion heading "New Pampers are HORRIBLE!" (The discussion thread is no longer available online.) Pampers responded to those concerns. Here is an exchange (with the names changed):

Debbie: I know I'm going to get a lot of flak for this, but oh well. I want to let people know my experience.

I've been using Pampers on my daughter since she was born in Oct. 08. I never had a problem with them and LOVED them. The softness of them was what made me use them at first. Then it was the absorbency. My daughter has sensitive skin and everything else made her breakout besides Pampers and Huggies. And I didn't like Huggies because of the stiffness.

When the new Pampers came out Sarah was wearing the Cruisers and I had no clue they changed. I bought a box and it looked EXACTLY the same as the ones I was buying before. When we opened the box to start using them we noticed right away that they were different. They were REALLY thin and didn't feel as soft, but I tried them anyway.

Sarah started getting rashes RIGHT away. And when I say rashes, I mean

(Continued)

(Continued)

REALLY BAD rashes. I change her right when I notice she's gone. Usually a minute or two after she's gone because I know her cues. Her rashes were blistering and bleeding. And when I'd get them to clear up they'd come right back. I started asking around and found out a LOT of people were having the same problem with their children.

We switched over to Huggies Little Movers and Huggies Overnight and we haven't had rashes like that since.

To the pampers people: You REALLY need to look into this. This is NOT an isolated problem. It's happening to a LOT of parents.

Pampers: Hi Debbie. You definitely won't get flak from us for sharing your experience. We appreciate it, but I'm just so sorry to hear about Sarah's rashes, as well as Maria's children and Bridget's baby.

Please do understand that we thoroughly evaluate our diapers to ensure they are safe and gentle on your little one's skin. Although I'll be passing this information along to our Health & Safety Division, I really hope that you, Bridget, and Maria get in touch with us directly at 1-866-586-5654. We're available M–F, 9–6, EST.

Shelley—I'll be sure to share your feedback with our Quality Control Team. We'd love you to give them another try since you had trouble with the tabs. Just get in touch with us at the same number and we can offer some help.

Pampers was reaching out to people expressing their concerns via social media. Pampers even held a summit with four influential "mommy bloggers," women who blog about consumer products intended for family use: Renee Bigner, Kate Marsh Lord, Tiffany Snedaker, and Stephanie Manner Wagner. The summit was a chance for Pampers and independent experts to provide information about the situation and to dispel the rumor. The four bloggers agreed that after the meeting they had greater confidence in the diapers (Sewell, 2010). Managers do consider negative information appearing in social media as legitimate threats to the reputation of the organization, the reputation of products, and the sales of those products. In other words, social media can be a warning sign for a problem that has the opportunity to grow into a full-scale crisis.

it was only 8% effective at killing E. coli. In the lawsuits that followed the outbreak, Odwalla admitted to more than 300 reports of bacterial poisoning prior to the 1996 event. Moreover, the U.S. Army had denied Odwalla access to military commissaries. Just four months before the outbreak, Army inspectors found an unacceptably high bacteria count in its sample and decided the risk was too high to sell in commissaries (Entine, 1998, 1999). Had Odwalla taken the warning signs seriously and either changed to the chlorine wash or switched to flash pasteurization, the 1996 outbreak would probably not have occurred.

One important source of concern is public criticism of the organization. Heath (1988) recommends that "all public criticism should prompt corporate leaders and operations managers to conduct studies to determine whether the charges are true and whether

key publics are believing the allegations" (p. 105). Complaints can be found in inquiries customers make to an organization or protests from activists. Inquiries may reveal an actual problem or a rumor, as people call to confirm the information they heard. Consider Nestlé's online confrontation with Greenpeace and others concerned about rainforests.

In the spring of 2010, Greenpeace began a campaign designed to force Nestlé to stop sourcing palm oil from Sinar Mas and other suppliers that illegally destroy rainforests as part of their efforts to extract palm oil. The campaign featured orangutans because rainforest destruction threatens their existence. There were protests in Europe, with people dressed as orangutans, but it was the Internet where the public complaints were most active. People could visit the Greenpeace web page titled *Ask Nestlé to Give Rainforests a Break*, a play on the commercial jingle for the company's Kit Kat candy bar. The site provided information and a parody video of a Kit Kat commercial in which the pieces of the candy bar were orangutan fingers that dripped blood (Greenpeace, 2010). Even more impressive was the hijacking of Nestlé's Facebook page. Suddenly a little-noticed Facebook page was flooded with criticisms for the company's palm oil policies and killing of orangutans (Leonard, 2010). In March, Nestlé announced that by 2015 it would be using only certified-sustainable palm oil. But the public criticism continued and deemed Nestlé's action as too weak (Leonard, 2010). On May 17, 2010, Nestlé went further in response to its critics by announcing an alliance with the Forest Trust to develop responsible sourcing guidelines for palm oil and to help fight deforestation of the rainforests (Nestlé, 2013). Public pressure, amplified by social networking, created a crisis and forced Nestlé to change its palm oil policies.

Here's another example. Febreze is a fabric refresher manufactured by Procter & Gamble (P&G). One of its main selling points is its ability to eliminate pet odors. So when a rumor began circulating on the Internet that Febreze kills pets, there was reason for concern. Here is a sample message:

> There have been multiple instances of dogs and birds that have died or became very ill after being exposed to Febreze, a deodorizer/air freshener. Febreze contains zinc chloride, which is very dangerous for animals. Please do not use Febreze anywhere near your pets! If you have used it near your pets or on their bedding, clean the bedding area thoroughly to remove the Febreze, and move the animals away from the area. Please pass this information on to other pet owners/caretakers, before more animals are injured or killed, and find a safer method of odor control. (About.com, 2002, paras. 1–3)

P&G soon began receiving phone calls and emails asking if Febreze was safe around pets. The P&G response was "Yes!" The product had been tested and proven safe around dogs and cats. P&G created a special section of its Febreze website to debunk the myth. People were told of Febreze's safety and directed to testimonials from the National Animal Poison Control Center and the American Society for the Prevention of Cruelty to Animals (Snopes.com, 2011). P&G used the consumer concerns to fight the rumor and protect the sale of Febreze.

TABLE 3.1 ■ Potential Crisis Sources to Monitor

Issues Management Sources		
TRADITIONAL		
News media: newspapers, television news, news and business magazines		
Trade journals: medical and science journals		
Newsletters: government publications		
Public opinion polls: public opinion experts		
Stakeholder actions		
DIGITAL		
News and business wires		
Online newspapers, magazines, and trade publications		
Archives for professional associations, special interest groups, and government agencies		
Consumer-generated media: websites, blogs, and discussion groups		
Newsgroups		
Risk Assessment Sources		
Total quality management	Liability exposure	Natural disaster exposure
Environmental crisis exposure	Criminal exposure	Product-tampering exposure
Legal compliance audits	Financial audits	Ethical climate surveys
Workers compensation exposure	Safety, accident records	Behavioral profiling
Internet use monitoring		
Reputation Sources		
Stakeholder messages posted to websites, blogs, social media, and discussion groups		
Stakeholder comments sent to the organization		

ORIENT: COLLECT THE INFORMATION

Once potential environmental information sources are located, crisis managers face the challenge of gathering the information. Data scrapping or harvesting (extracting data from digital channels and platforms), interviews, surveys, focus groups, and informal contacts are among the most frequently used collection tools. Familiarity with these tools is an important crisis management asset.

The first step in soliciting information from stakeholders is for the crisis team to construct a stakeholder map that lists all possible stakeholders (Grunig & Repper, 1992). Box 3.2 presents sample stakeholder maps that HP and Tesco use to guide their stakeholder engagement effort. Then the crisis team would identify the stakeholders relevant to the most highly ranked crises. Interviews, surveys, focus groups, or key contacts can be used to collect information from stakeholders. Interviewers ask people questions about a particular subject in an organized fashion. The interviewers develop and follow an interview schedule. Preparation is essential. The person collecting the information must have an organized approach to the interview if it is to yield useful information (Stewart & Cash, 1997). Surveys collect information about people's perceptions, attitudes, and opinions. Surveys can be conducted by having people complete questionnaires or by having researchers ask stakeholders the questions. Focus groups are collections of specific stakeholders who are brought together to listen to and respond to questions as a group. Open-ended questions are used to encourage interaction and to probe the nature of people's beliefs. Key contacts are community, industry, or organization leaders who are selected because of their expertise on a subject. Using public opinion or issue experts is a form of key contact (Baskin & Aronoff, 1988).

BOX 3.2

SAMPLE STAKEHOLDER MAPS

HP

Stakeholder engagement is integral to global citizenship, and HP works to build strong, mutually productive relationships with our diverse stakeholders. They include

- Communities
- Customers
- Employees
- Investors
- Legislators and regulators
- Industry analysts and media
- Nongovernmental organizations (NGOs)
- Suppliers
- Universities (HP FY07, 2008)

Tesco

- Customers
- Employees
- Investors
- Communities
- Suppliers
- Governments and regulators
- Nongovernmental organizations (Canadian Imperial Bank of Commerce, n.d.)

ORIENT: ANALYZE THE INFORMATION

Collecting information about issues, risks, and stakeholder relationships is of no value unless the information is analyzed to determine whether it contains crisis risks. Analyzing information creates knowledge (Geraghty & Desouza, 2005). Crisis managers

determine whether the information really does suggest a possible crisis—whether or not a red flag exists. The premise behind finding warning signs early is to locate those that can significantly impact the organization and to take action to manage them (Dutton & Duncan, 1987; Gonzalez-Herrero & Pratt, 1996; Heath & Nelson, 1986). Analysis is the process of understanding if and how a warning sign might impact the organization (Heath & Nelson, 1986). Crisis managers need criteria for evaluating issues, risks, and reputation threats.

When utilizing any print, online, or broadcast source, content analysis can be useful. It involves the systematic coding and classification of written materials, be they news stories, articles in other publications, or transcripts of focus groups or interviews. Effective content analysis requires the development of coding categories and expertise in using the categories. Coding categories are the boxes in which discrete pieces of information are placed. Each category needs a thorough written definition that indicates what is appropriate for it, and these categories must be mutually exclusive—no message should fit into more than one category (Stacks, 2002; Stewart, 2002). People who use the categories, the coders, must be trained in their use. Coders must be able to place similar messages in the same categories. This consistency is called *reliability*. Reliability allows different people to code messages consistently. Such consistency allows for comparisons of the coded data. Content analysis converts the written information into quantifiable data—the words become numbers that can be analyzed using statistics. Some examples may help to clarify the content analysis process.

Most organizations have established categories for accidents and safety violations. People are trained to understand the differences in the accident and safety categories so that they can accurately record these events. An organization can examine the data to see if certain accidents or safety violations have increased or decreased over time. For example, an organization might be interested in the number of falls in a particular area of the organization. Systematic coding of accidents permits an accurate analysis of the fall data. Similarly, organizations should develop categories for coding customer complaints. It is not enough to know the sheer number of complaints received; organizations should know the type and frequency of different varieties of complaints. By categorizing customer complaints, organizations can identify problem areas by the increase of complaints in those areas. If an airline receives increasing complaints about how canceled flights are handled, it needs to improve its customer service relative to canceled flights. Systematic coding allows for comparisons that could not be made if the written information had not been quantified. It is the recording and quantifying of the material that qualifies content analysis as a form of information collecting.

More and more we find content analysis being conducted by computers. The computer-based content analysis is helpful in identifying key words, sentiment, and frames in crisis messages (van der Meer, 2016a, 2016b). Key words can be indicators of a risk or crisis. Examples would be mentions of a product defect or people getting sick from a particular food. When certain crisis- or risk-related key words begin to trend, that is a red flag. Sentiment analysis indicates if the messages are positive or negative for an organization. The Red Cross usually has only a 10% negative sentiment, thus when it suddenly jumped to 80%, the organization knew it had a problem (DC Communicators, 2017). By looking at the content of the messages, the Red Cross learned concerns over a pool safety poster being racist was the cause of the crisis. After carefully examining the

situation, the Red Cross took action to address the crisis. Other metrics that can be used to analyze the data are total mentions (aggregate of mentions about an organization or product), total impressions (potential audience reached by the messages), and duration of the digital discussion. I would argue these are preliminary steps in your crisis and risk assessment. The final step is an actual threat assessment.

We can build threat assessment analysis around two factors: likelihood and impact. Likelihood is the probability that a threat will become a crisis. Impact is the effect the crisis can have on stakeholders and the organization. Typically, each threat is given a score from 1 to 10 for likelihood and threat, with 1 being low and 10 high. When crisis managers analyze the issue, risk, and reputation threats in terms of likelihood and impact, they can determine whether each threat warrants further attention and/or action. Likelihood and impact have slightly different meanings for the issues, risk, and reputation.

For issues, likelihood is the probability of an issue gaining momentum. An issue with momentum is developing and is more likely to affect the organization. Some indicators of momentum are sophisticated promotion of the issue, heavy mass media coverage, strong Internet presence, and a strong self-interest link between an issue and stakeholders. The 1989 anti-Alar campaign illustrates an issue with momentum. Alar is a chemical that was used to treat apples. Within a year of launching its campaign, the anti-Alar coalition headed by the Natural Resources Defense Council (NRDC) had caused Alar to be removed from use. The Alar issue had professionals crafting the publicity effort: sophisticated promotion. Celebrity appearances, including from Meryl Streep, helped to garner massive publicity: heavy media coverage. And Alar was treated as a threat to innocent children: a strong self-interest link between Alar and consumers (Center & Jackson, 1995).

Impact refers to how strongly the issue can affect profits, reputations, or operations. It involves the use of forecasting, which projects the potential effect of an issue on the organization. There are at least 150 forecasting techniques used in business. A detailed discussion of forecasting is beyond the scope of this book, but Coates, Coates, Jarratt, and Heinz (1986); Ewing (1979); and Heath (1997) offer more details on forecasting techniques. Organizations should use those forecasting methods with which they are familiar. Only issues with high impact would be considered crises because a crisis must be disruptive to organizational operations.

For risks, likelihood is the probability that the risk can or will become an event—the risk will cause something to happen. This estimates the possibility of the risk being exploited or maturing into an event. Impact is, again, how much the event might impact the organization and its stakeholders. In this context, it includes disruption to organizational routines and potential damage to people, facilities, processes, or reputation (Levitt, 1997).

For reputation, the evaluation of likelihood and impact is not as clearly developed and is a little more complex. Before evaluating likelihood and impact, crisis managers must determine if an expectation gap exists. As noted earlier, reputations are built around stakeholder expectations. Different stakeholder groups will have different expectations for organizational behaviors. For instance, investors want the organization to make money, employees want adequate pay and medical benefits, and community groups want the organization to be engaged in the life of the community. The point is that crisis managers must identify the expectations held by each major stakeholder group. Through research, they can isolate stakeholder expectations.

Once the expectations are known, crisis managers must determine whether the stakeholders perceive the organization as meeting those expectations; they search for gaps. Figure 3.1 illustrates two types of gaps. The first is based on performance; the organization is not doing what it needs to do to meet expectations. The second occurs when stakeholders fail to perceive that the organization is meeting expectations. Perception is the key. Even if an organization has made significant efforts to reduce pollution, if the stakeholders do not know about it, there is a gap.

If stakeholders have concerns based on expectation gaps, the stakeholders can become a reputation threat by taking action against the organization and generating negative publicity. That threat is intensified by the various digital communication channels and platforms (Conway, Ward, Lewis, & Bernhardt, 2007). Not all expectation gaps lead to crises. Moreover, no organization has the time, money, or personnel to address every expectation gap. So what is an organization to do? The answer is to prioritize stakeholders and focus your resources on those that have the greatest potential to initiate crises. Crisis managers must be able to differentiate between mild and serious threats. The challenge is how to determine the likelihood and impact of an expectations gap. One option is to examine the salience of the stakeholder involved in the expectation gap. Stakeholder salience, their importance to the organization, can then be converted into likelihood and impact scores. Stakeholder salience is a function of power, legitimacy, and willingness.

Power is the ability of the stakeholder to get the organization to do something it would not do otherwise. Power relates to the stakeholder's ability to disrupt organizational operations. Stakeholders who control essential resources or can form coalitions have strong power. Control over essential resources permits a stakeholder to disrupt organizational processes. For instance, employees can stop the production process or the delivery of goods and services. As mentioned earlier, in 1997, UPS drivers launched a strike that crippled the company's ability to deliver its primary service.

Coalition formation supplies power through numbers. As stakeholders join forces with one another, their power increases (Mitchell, Agle, & Wood, 1997; Rowley, 1997). An example would be an activist group that persuades shareholders and customers to join its efforts to pressure an organization for change. The combination of activists, customers, and shareholders was instrumental in convincing Levi Strauss to close its production facilities in Myanmar. Activists persuaded customers and shareholders that facilities in Myanmar contributed to human rights violations there. In turn, customers and shareholders questioned Levi Strauss's operations there. Levi Strauss felt that the stigma of human rights abuse was reason enough to leave Myanmar (Cooper, 1997). The Killer Coke campaign has followed a similar strategy. Alone, the activists would have little impact, but combined with shareholders and customers, they can exercise great power.

Stakeholder power is enhanced by the ability to take action against the organization. Stakeholders need resources (e.g., money) and skill in using communication channels if they are to put pressure on an organization (Ryan, 1991). Let us return to the NRDC's effort to ban Alar. The NRDC had money to hire professional communicators to develop a major publicity campaign promoting the danger of Alar. The campaign raised awareness of Alar danger from 0% to 95% in less than a month (Center & Jackson, 1995). Money and publicity skills created the perception of Alar as a cancer threat to children.

Legitimacy refers to actions that are considered desirable, proper, or appropriate according to some system. A stakeholder concern is more serious when it is deemed

legitimate by other stakeholders. If other stakeholders see a concern as legitimate, they are likely to support the need to take action. Illegitimate issues are easy for other stakeholders to ignore because they are considered inappropriate or unimportant. Ignoring a legitimate concern makes the organization appear callous to the other stakeholders. They ask, "Why doesn't the organization address this reasonable concern?" Offending other stakeholders increases the risk of the threat spreading to additional organization–stakeholder relationships. Crisis managers should determine whether other stakeholders will view the concern as legitimate. This requires knowing the values and social responsibility expectations of various stakeholder groups (Mitchell et al., 1997).

Willingness refers to stakeholders' desire to confront the organization about the problem. A problem must be important for them, and their relationship to the organization must be relatively weak. Importance prompts stakeholders to take action. Why push a problem if it is unimportant? And stakeholders are less likely to pursue a problem when they have a favorable relationship with the organization. Once more, the Alar case illustrates the point. The NRDC considered Alar to be salient; it was the group's major concern at the time. The NRDC seemed to have no real relationship with the apple growers, the group affected most by the anti-Alar campaign. Documentation of the case makes no mention of the two sides ever meeting to discuss the concern prior to the launch of the NRDC's anti-Alar publicity campaign (Center & Jackson, 1995). A favorable relationship encourages both sides to seek a nonconfrontational approach to problem-solving (Grunig & Repper, 1992).

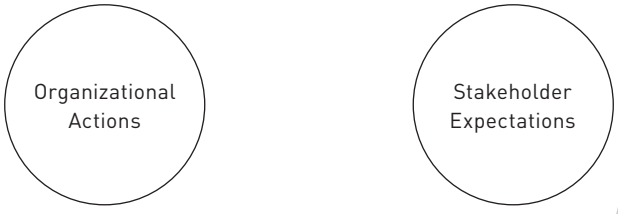
Let us return to the Greenpeace–Nestlé palm oil case to illustrate power, legitimacy, and willingness. Greenpeace is an important activist organization that generated power by hijacking Nestlé's Facebook page and generating negative traditional media coverage and social media comments. Nestlé could not ignore the public relations pressure. Other stakeholders supported Greenpeace because the concern was legitimate. Most people feel we should protect the rainforests. Greenpeace's communication efforts showed it was willing to exert pressure about the issue. Even after Nestlé made minimal effort to address the problem initially, Greenpeace kept the pressure on for two more months until there was significant movement on the deforestation concern.

Power, legitimacy, and willingness can be translated into impact and likelihood. High power and legitimacy indicate a strong impact. Stakeholders can disrupt the organization and are likely to be perceived by others as having a valid (legitimate) reason for doing so. Therefore, power and legitimacy can be used to establish an impact score. Legitimacy and willingness suggest a strong likelihood of occurrence. Willingness increases the chance of a stakeholder taking action, while legitimacy increases the possibility of other stakeholders supporting the action. Thus, legitimacy and willingness can be used to establish a likelihood score.

At this point, it is instructive to return to sentiment analysis to demonstrate how the initial assessment of data can aid in threat assessment. Sentiment analysis assigns a quantitative positive/negative mood score to text. The process involves detecting, extracting, and classifying the sentiment that appears in text. Sentiment analysis is a method that is used in subjectivity analysis. Subjectivity analysis seeks to detect "private states," such as emotions and sentiments. Sentiment analysis is a means of deriving private states from text (Montoyo, Martinez-Barco, & Balahur, 2012). One of the pieces of critical information found on dashboards provided by social media monitoring companies is sentiment

FIGURE 3.1 ■ Expectation Gaps

Performance Gap: Organizational actions do not match stakeholder expectations



Perception Gap: Organizational actions do match stakeholder expectations, but stakeholders do not perceive the match

analysis. In most cases, the sentiment analysis is derived from a computer analysis of social media messages. It is important to note that there are questions about the accuracy of these automated content analyses. Automated coding has been shown to have only a 60% to 80% accuracy level compared to human coding (Mullich, 2012). However, the analyses are accurate enough to be of value to crisis managers, and the companies keep working to improve the accuracy (Sterne, 2010).

Summary

By assessing the threat information, crisis managers create knowledge. That knowledge is an understanding of how important each threat might be to the organization. We can refine crisis threat assessment by creating a formula for calculating crisis threat values: crisis threat = likelihood x organizational impact x stakeholder impact. For those who like abbreviations, we can write the formula as CT = L x OI x SI. Earlier in this chapter, issue and risk impact were noted as involving both stakeholders and organizations. Crisis

managers should think of both types of impact when assessing a crisis threat. A running theme in this book is the primary importance of stakeholder safety during a crisis. By incorporating stakeholder impact into crisis threat assessments, we further honor the commitment to stakeholder safety.

Combined, the first three steps in crisis prevention form the crisis-sensing mechanism, a systematic means of collecting crisis risk information that is built on three points: (1) locating the source of crisis risk information, (2) funneling the information to a central location, and (3) making sure the information is analyzed—converted into knowledge. Sources, collection tools, and evaluation criteria are the raw materials used to construct the crisis-sensing mechanism—the crisis radar and tracking system. No one crisis-sensing mechanism is right for all organizations. Each organization has quirks that must be accommodated, but some basic ideas can be offered.

The crisis-sensing mechanism can be viewed as knowledge management (KM). It finds and shares what is known by an organization or its external stakeholders. KM differentiates between *information* and *knowledge.* Information simply places facts in context, while knowledge analyzes the information so that it is usable by people in the organization (McKeen, Zack, & Singh, 2006; Rollins & Halinen, 2005). There is a close connection between KM and some aspects of crisis management; knowledge is essential to all phases of crisis management. In fact, "managing knowledge well is key to enhancing an organization's ability to deal with business crises" (Wang & Belardo, 2005, p. 7).

The crisis-sensing mechanism, a KM strategy, is a means of finding the knowledge an organization needs (Wang & Belardo, 2005). It attempts to create a repository of warning sign knowledge by locating, collating, and analyzing the crisis risk information or existing crisis knowledge.

Crisis sensing begins by determining what information-sensing mechanisms already exist in your organization. Avoid recreating the wheel. Review the issue management sources, risk sources, and reputation sources to see if they are comprehensive. Find out where your organization currently collects warning sign–related information or already processes it into knowledge. New procedures should be developed only if key sources are being overlooked. For instance, if no efforts are being made to scan relevant activist groups, add that as a source. A similar review should be undertaken for information-gathering techniques. Keep in mind that if you have the financial resources, you can hire vendors to help you scan, especially for issue and reputation information. Pay particular attention to how information and knowledge, such as publicity, are coded. A common weakness in information collection is a coding system that is too general and misses important details contained in the information (Denbow & Culbertson, 1985).

Consider this example that illustrates the importance of details. Let's say a retail store tracks its media coverage by collecting and analyzing news stories about and social media mentions of the organization. A general coding system might simply count the total number of positive and negative comments about the retail store. The analysis provides a global evaluation of the reputation: Is it favorable or unfavorable? No insight is provided into why the media image is favorable or unfavorable. A more specific coding system might include the following categories: sales staff, customer service, selection, merchandise quality, value and pricing, store appearance, and parking. The retail store would have separate evaluations for the seven categories. Store managers would know the exact areas where the store's image was strong and where it needed improvement.

Second, the organization must establish mechanisms and procedures for funneling relevant information and knowledge to the crisis manager or the crisis department. An organization should have at least one person who is dedicated full-time to crisis management (Coombs, 2006a). Crisis sensing is easier if there is an entire department, but many organizations are lucky to have one crisis manager. Crisis managers cannot process information they have not received nor attend to warning signs (knowledge) never encountered. Crisis managers must receive the scanning information and knowledge in a timely fashion and must carefully analyze the information for the warning signs. Various areas of the organization and possibly some vendors are likely to be responsible for different pieces of internal information and knowledge. Some organization units involved in scanning include operations and manufacturing, marketing and sales, finance, human resources, legal, customer communications and satisfaction, environmental and safety engineering, public relations and public affairs, engineering, ping and distribution, security, and quality assurance.

The many organization units and vendors hired to scan must send this information and knowledge to the crisis team as soon as possible after they first receive and evaluate the information. The crisis manager becomes the center of a larger crisis-sensing mechanism. He or she must act as a functioning unit that is integrated within the flow of organizational activities, information, and knowledge exchange. Channeling information and knowledge sounds easier than it is. Consider that most organizations have difficulty collecting and analyzing information from customers (Rollins & Halinen, 2005). Now add information from a number of additional stakeholders, and your crisis-sensing mechanism becomes a real challenge.

Third, the crisis manager's assessment criteria for warning sign–related information must be carefully developed. This discussion provides general criteria for assessing issues, risks, and reputation threats. Crisis managers may wish to add their own organization-specific assessment criteria. The crisis team must determine which criteria they would like to use, develop additional criteria if need be, and determine precise definitions for the assessment criteria. Without precise definitions, the crisis manager is not able to apply the assessment criteria consistently. Last, the crisis-sensing mechanism must be tested to determine whether the various parts are integrated effectively. Running carefully selected and controlled information through the system is one way to assess the integration's effectiveness.

Walmart, for instance, has a crisis-sensing mechanism for staying ahead of crises. Jason Jackson, Walmart's director of emergency management, uses what he terms *watchdog positions.* The watchdogs monitor a variety of sources, including the Internet, news reports, and information from local stores, to identify possible disruptions to business. One source they monitor is weather, and hurricane Katrina stands as testimony to the value of weather scanning. Before Katrina made landfall, Walmart had 45 trucks loaded with essential supplies ready for delivery. As Barbaro and Gillis (2005) comment, "Wal-Mart is being held up as a model for logistical efficiency and nimble disaster planning, which have allowed it to quickly deliver staples such as water, fuel and toilet paper to thousands of evacuees" (para. 4). When watchdogs find a threat, they relay that information to the emergency management team. The emergency management team evaluates the information and decides what action, if any, should be taken. Johnson conducts regular training and testing of Walmart's system (Rojas, 2006). The Walmart watchdogs concentrate on risk management and operational concerns, such as weather and security.

However, Walmart's crisis-sensing mechanism had not been tuned to issues management and reputation management. In 2005 and 2006, the company moved to improve both of these aspects through the hiring of external agencies and internal personnel. Walmart also launched its first-ever reputation advertising campaign around this time period. This effort was designed to shore up the company's reputation with customers and employees (Hays, 2003). However, these issues management and reputation management efforts are not connected with the risk management efforts to build a comprehensive crisis-sensing mechanism. Walmart has been expanding and improving its crisis-sensing mechanism by capturing digital platforms. In addition to using the Brandwatch software, Walmart utilizes searches, Twitter lists, and basic listening to monitor social media platforms for red flags (Joffe, 2018).

Crisis sensing can seem daunting, especially considering the need to scan so many sources. Organizations that can afford it can find assistance from monitoring services, which now cover traditional media and the Internet, including social media. Prominent monitoring services include BurrellesLuce, CyberAlert, and dna13. These companies aid in finding, retrieving, and even analyzing media, a large part of the external threat sources.

DECIDE AND ACT: TAKE PREVENTIVE ACTION

Once threats have been evaluated, crisis managers determine whether to take action. Many threats are too minor and can be ignored. Crisis managers must determine what actions to take on the serious threats. One option is to monitor the threat if it does not pose an immediate danger. Monitoring involves following the development of the warning signs. The crisis team continuously collects and analyzes information about the warning signs, looking for changes that indicate whether the risk is becoming more or less likely to evolve into a crisis. The information sources, collection tools, and analytic criteria used in scanning are employed in monitoring. The key differences are a search for more detailed information and the continuous application of the search process in monitoring.

If a threat is serious enough, action is taken to diffuse it. Actions create changes that eliminate or reduce the likelihood of a warning sign becoming a crisis. Actions are taken to manage issues, to reduce risks, and to build or maintain reputations. A few examples will illustrate this point. Say that the issues management unit of a company learns of a proposal to tighten air quality standards. Action is taken to prevent or postpone the new regulation, thereby averting a possible plant closing while the plant implements ways to reduce emissions. Or a safety review finds that workers are not following the unloading directions for hazardous chemicals. A refresher training course is offered along with new, stricter safety procedures regulating the unloading of chemicals. The risk of a hazardous materials accident is reduced. And here is another example: A number of complaints appear online about chain guards falling off of a chain saw. Customers are offered replacements and design changes are made to prevent the guards from falling off. Accidents and a major conflict with customers are averted, and the reputation is maintained.

In 2017, a gunman staying in the Mandalay Bay Hotel and Casino opened fire on people attending a music festival. The shooting resulted in 58 deaths and over 800 injured. The gunman had stockpiled weapons and ammunition and hid the stockpile from hotel personnel. Four Walt Disney World resorts were among the hotels to institute a new policy of entering rooms daily. The rooms have new signs that say "occupied" rather than "do not disturb" and hotel personnel will enter the room once a day even if the sign is on the door. The idea was to prevent a similar incident by not allowing guests to hide from hotel personnel ("Hotels Revise Room Security," 2018). In 2013, there were high-profile hacks to the Twitter accounts of Burger King and Jeep. While social media crises for Burger King and Jeep, the situations were more of a traditional crisis for Twitter. Organizations using Twitter were concerned their accounts could be hacked next—there was an operational concern. In May 2013, Twitter took action to reduce the likelihood of hacking by strengthening login verification with a form of two-factor authentication. Knowing no system is perfect, Twitter warned, "Of course, even with this new security option turned on, it's still important for you to use a strong password and follow the rest of our advice for keeping your account secure" (O'Leary, 2013, para. 4). The exact nature of the action will depend on the nature of the threat and best options for trying to reduce or eliminate that threat.

EVALUATE THE EFFECTIVENESS OF THE THREAT REDUCTION

Evaluation monitors the threat to determine whether the action taken to address it had any effect. Without monitoring, the organization does not know if the change has been effective—has it reduced or eliminated the chance of a crisis? For example, an organization would want to know whether the new safety procedures and policies made the workplace less hazardous. The only way to know if safety has improved is to monitor workplace behaviors. If workers are now engaging in safer behavior—fewer violations of safety procedures—then the safety changes are working. Never assume any change is for the better. Some changes produce no results, while others may intensify the warning signs or risks, thereby moving an organization closer to a crisis. Monitoring involves a regular review of any changes designed to reduce warning signs. The review determines the effectiveness of the changes and whether any additional modifications are warranted (Pauchant & Mitroff, 1992). Each threat reduction effort will pose its own unique demands for assessing its effectiveness by answering the question "Did you reduce the threat?"

Evaluating issues management depends on the goals of the issues management effort. Crisis managers must determine how close the final action taken on the issue was to the desired outcome for the issue. Crisis managers might be trying to prevent the government from taking action on an issue or trying to shape the policy being created to address the issue. Issues are cyclical and frequently do re-emerge (Crable & Vibbert, 1985). For instance, healthcare reform has been an issue in the 1940s, the 1950s, the 1990s, and multiple years since 2000. Part of the evaluation should consider if there are still groups actively seeking to manage the issue.

The evaluation of risk management—risk aversion, to be more specific—is an ongoing concern. Periodic reviews of the risk are conducted to determine the effectiveness of the risk aversion program (Pauchant & Mitroff, 1992). Evaluation compares the level of risk before and after the risk aversion program is implemented. The review is continued to determine whether the program works over time. Was the risk reduction a statistical aberration, or has the lower level of risk been maintained over the course of the program? The risk must be monitored continually to ensure that the threat does not reemerge.

For specific problems, stakeholders have stated what the concern is and have probably offered advice on how to solve the problem. If the organization decides to take action, management should ask the disgruntled stakeholders if the resolution was satisfactory. The feedback from stakeholders will serve as the measure of success.

Success in closing an expectation gap is determined by whether stakeholders perceive the organization as meeting expectations. The organization and stakeholders must co-create meaning—they must share a similar interpretation of the organization's performance on the desired expectations—for expectation gaps to be closed (Botan & Taylor, 2004). The most effective way to determine whether an expectation gap has been closed is to use surveys to assess stakeholder perceptions of expectation performance before and after efforts are initiated to close the gap. The survey provides the evaluative data necessary to determine whether stakeholder perceptions have changed. For example, one item can ask stakeholders to rate on a scale of 1 to 7 (7 being the highest), "Does the organization reflect your concern for the environment?" If the original evaluation was 2.5, a post-communication effort score of 4 would be considered a success, indicating that stakeholders see greater similarities between their concerns and the organization's behavior. Correctly identifying expectation gaps is the focus of organizational issues management, so the same evaluation method would apply to it as well.

Paracrises: A Review of Action and Evaluation

Paracrises emerge when an organization must manage a crisis threat in full view of its stakeholders. The crisis threat is made public, and people can see if and how the organization responds to the crisis threat (Coombs, 2017b; Coombs & Holladay, 2012c). The challenge "crisis" is a common form of paracrisis. A challenge paracrisis occurs when stakeholders publicly claim an organization is acting in an irresponsible manner. The earlier example of Greenpeace questioning the palm oil sourcing practices of Nestlé is a challenge paracrisis. Greenpeace was defining Nestlé's palm oil sourcing as irresponsible. The challenge is a crisis threat because it threatens Nestlé's reputation. As noted in Chapter 2, CSR can be a crisis risk when charges of irresponsibility are accepted by stakeholders, thereby damaging the organization's reputation (Coombs & Holladay, 2015).

When confronted with a challenge paracrisis, crisis managers have two decisions to make. First, should the organization address the challenge? Second, how should the organization respond to the challenge if the decision is to respond? Crisis managers have six basic responses to a challenge paracrisis: (1) refusal, ignore the challenge and choose not to respond; (2) refutation, argue that the organization's actions or policies are responsible and appropriate; (3) repression, try to silence the challengers by preventing them from creating and spreading messages; (4) recognition/reception,

acknowledge there is a problem but take no actions to address the problem; (5) revision, make some changes to the policies or behaviors but not the exact changes requested by the challengers, and (6) reform, make the changes to policies or behaviors requested by the challengers. The respond option selection depends on how powerful/threatening the challengers appear, the cost of the changes, and how consistent the change is with the organization's strategy. For instance, crisis managers are much more likely to engage in reform or revise when the cost of the change is low, the change is consistent with the organization's strategy, and the challenger is perceived as a threat (Coombs, 2017a; Coombs & Holladay, 2015).

The challengers provide a means of assessing the effectiveness of the paracrisis response in reducing the threat. If challengers end the challenge, the threat is reduced. If challengers escalate the challenge and successfully recruit other stakeholders to view the organization as irresponsible, the threat reduction has failed (Coombs, 2017a). The challenge paracrisis illustrates how a crisis threat can be identified, a decision made on how to address the threat, and a means of evaluating the threat reduction provided.

WHAT WOULD YOU DO?

EGOS MOBIL PHONE ADVERTISEMENT

You work for Egos Mobil Phones, a company that was once independent but is now owned by Sprint. The company kept the name "Egos" because it was a very recognizable brand. Egos Mobil was once part of business empire of celebrity CEO James Egos. He sold the company two years ago to Sprint. It is December 10 and Egos has begun running a number of online advertisements. The campaign is edgy with hopes of some of the short advertisements going viral. One advertisement does generate buzz online but not in a good way. The video shows a man covering a woman's eyes with the caption "The gift of Christmas surprise. Necklace? Or chloroform?" Many people find the advertisement tasteless and seemingly to indirectly support rape. People express their displeasure online. Negative comments are even posted to James Egos's blog. Egos condemns the advertisement on his blog.

- What advice would you give to Egos management about how to respond to the situation?
- Would you consider this a paracrisis or crisis? What led you to your choice?

Crisis Leadership Competencies: Risk Taking

Crisis leaders should be open to trying new things and to unconventional thinking. A danger when scanning for crisis threats is that managers may respond negatively when they do find a threat. The threat-rigidity phenomenon says that people are more conservative and restrictive with sharing information as a threat intensifies. Leaders need to prevent crisis threats from triggering rigidity (James & Wooten, 2010). Leaders must emphasize the need to not only find crisis threats but share that information with others and attempt solutions designed to reduce the likelihood of a threat becoming a crisis. The crisis leadership competencies of sense making and creativity are important for prevention as well. Sense making helps leaders interpret the warning signs, while creativity aids in anticipating how the threat might develop and impact both the organization and its stakeholders.

CONCLUSION

A crisis prevention program is a valuable part of the crisis management process. The crisis team uses the warning signs from signal detection to target situations that could become crises. The team then takes actions designed to eliminate or reduce the likelihood of the warning signs developing into crises. As Paine (2011) states so eloquently, "The single best way to avoid a crisis is to listen carefully to your audiences and respond to threats *before* they get out of hand" (p. 165).

But prevention is not as easy as it sounds. Finding potential crises is a type of warning environment, and a warning environment involves ambiguous information and penalties for incorrect actions. Possible crises can be hard to detect, and failure to do so can result in a crisis. Unfortunately, organizational politics can complicate or even block efforts to reduce risks. (Chapter 6 offers suggestions for combating resistance to preventative actions.)

Ideally, crisis teams must remember to monitor their corrective actions on a regular basis to determine whether preventative actions have produced the desired effects. However, an organization cannot count on avoiding all crises. Hence, the need remains for crisis preparation, which is the subject of Chapters 4 and 5.

DISCUSSION QUESTIONS

1. Locate and read information about fair-trade coffee. Do you think it is an idea that will gain additional support among coffee growers? Is Starbucks wise to increase its support for fair-trade coffee?
2. What barriers do you see to organizations taking preventative measures? How might they be overcome?
3. What are some organizational barriers to creating a crisis-sensing mechanism? How might you overcome those barriers?
4. How is social media changing crisis prevention efforts?
5. What recommendations would you make to a small organization about how best to monitor the online environment?
6. Does it make sense to distinguish between traditional websites and social media, or should we treat all online communication channels and platforms the same?
7. Why is it useful to include impact evaluations for both stakeholders and organizations?
8. Why should managers bother identifying red flags?
9. Why could you consider paracrises both risks and opportunities?