Code Red in the Boardroom: Crisis Management as Organizational DNA

W. Timothy Coombs

PRAEGER

Code Red in the Boardroom

Code Red in the Boardroom

Crisis Management as Organizational DNA

W. Timothy Coombs

PRAEGER

Westport, Connecticut
London

Library of Congress Cataloging-in-Publication Data

Coombs, W. Timothy.
Code red in the boardroom : crisis management as organizational DNA / W. Timothy Coombs.
p. cm.
Includes bibliographical references and index.
ISBN 0-275-98912-7 (alk. paper)
1. Crisis management. 2. Communication in management. I. Title.
HD49.C663 2006
658.4'056—dc22 2005034113

British Library Cataloguing in Publication Data is available.

Library of Congress Catalog Card Number: 2005034113
ISBN: 0-275-98912-7

First published in 2006

Praeger Publishers, 88 Post Road West, Westport, CT 06881
An imprint of Greenwood Publishing Group, Inc.
www.praeger.com

Printed in the United States of America

The paper used in this book complies with the Permanent Paper Standard issued by the National Information Standards Organization (Z39.48-1984).

10 9 8 7 6 5 4 3 2 1

To Sherry, for all her support with this project,
and to Mac, for being himself.

Contents

Preface

Read or watch the news and you know that organizations face crises every day. Some are small, and some are mammoth, but all can harm the unprepared organization. Crisis management is more than just a document. Throughout this book, I argue that true crisis management involves making it a part of the organization's DNA. Crisis management is what an organization *does*, not something it has. Great crisis managers know that the best way to manage a crisis is to avoid one. However, not all crises can be prevented, so managers must be prepared to deal with the reality that crisis is a matter of when, not if. The purpose of this book is to reinforce the need for crisis management and push organizations to make it a part of their DNA. Part I examines the main types of crises to illustrate the daily threats an organization may face. Part II provides advice on managing crisis and integrating crisis management into the organization's DNA. The appendixes provide additional practical tools and resources.

1

Introduction: Crises Do Happen, So Be Prepared

Since the terrorist attacks of September 11, 2001, American companies have been more aware that the world is a dangerous place. Even the best company is just a few steps away from a crisis. Companies should be prepared through crisis management. Unfortunately, the preparation is often more talk than action. Management takes a few surface actions and believes their company is ready to face a crisis. Or worse, only a few actions are taken because management thinks a crisis will not happen to them. To be effective, management must take crisis management seriously. Crisis management is not an extra to be *added on*. It needs to be something that an organization *is*. I refer to this as crisis management becoming part of a company's DNA. This chapter reviews the need for crisis management and the difference between crisis management as an add-on verses crisis management as DNA.

CRISES: DEFINITION AND DANGERS

We often use the term *crisis* lightly. It is a crisis when we misplace our keys, or the toner in the copier runs low. In corporate life, the

word *crisis* should be reserved for specific events. A crisis is an unpredictable, major threat that can have a negative effect on the organization, industry, or stakeholders if handled improperly. Although we can anticipate that crises will occur, we do not know when they will happen. Crises are like an earthquake. We know one can hit but cannot predict exactly when. Crises threaten to disrupt a company's operation or demand significant resources—it is a major threat. Crises can result in negative outcomes, such as injuries, loss of life, loss of financial resources, property damage, environmental damage, and reputational damage.[1]

Humans are good at ignoring threats. We choose to ignore that certain actions, such as eating fatty foods, can cause health problems. Why do people still smoke or drink and drive when the dangers are well known? Management is only human and can choose to ignore that the company has crisis risks. In reality, companies are vulnerable to a wide array of crises. We can categorize crises into three groups: (1) attacks on an organization, (2) accidental actions that place stakeholders at risk, and (3) purposeful wrongdoing by management. A few examples will illustrate the vulnerability of companies to these types of crises.

In late 1999, Burger King ran a tie-in promotion with the popular cartoon and trading card game Pokémon. This was a marketing coup for Burger King, as the giveaway was a magnet attracting millions of children to the restaurants. In December, the joy turned to sorrow. On December 11, 1999, a thirteen-month-old girl in Sonora, CA, was found suffocated in her playpen by half of a Poke Ball (part of the giveaway). On December 27, Burger King announced the recall of the Poke Balls. The recall effort included full-page advertisements in *USA Today*. In January 2000, a four-month-old boy in Indianapolis suffocated in his crib because of a Poke Ball. Burger King intensified the recall with fifteen-second television advertisements. The recall effort was well beyond the government-required distribution of news releases. Experts speculated on its effects on Burger King's reputation and sales. Burger King maintained it had always informed consumers that the giveaways were for kids over the age of three.[2] However, this was little comfort in light of two deaths. Success of the tie-in quickly changed to a serious threat.

For most of 2004, a computer hacker had gained entry into wireless giant T-Mobile's servers. He accessed passwords, Social Security numbers, e-mail messages, and personal photos. Nicholas Jacobsen began selling people's identities, reading e-mails of U.S.

Secret Service agents using T-Mobile, and posting online personal photos taken by Hollywood celebrities Demi Moore, Paris Hilton, and Ashton Kutcher. The hack was known as early as March 2004. The government began active involvement with the case in July 2004 and began making arrests in October 2004.[3] T-Mobile was embarrassed by one hacker who had free rein through their sensitive data for over six months. T-Mobile, like most companies that were hacked, was reluctant to go to authorities for fear of public embarrassment and loss of customers.

Kinston, North Carolina, is the home to one of West Pharmaceutical's production facilities. That operation converts rubber into syringe plungers and intravenous fitments. The Kinston facility is brand new; it reopened in 2004. On January 29, 2003, an explosion leveled the old facility. There was no production for over a year. The greatest tragedy was not the destruction of the facility; it was the deaths of six employees. There is a permanent memorial to commemorate those workers. The cause of the accident was dust. Rubber dust had accumulated in a drop ceiling. Something ignited the dust, and the explosion leveled the facility. Any organic dust can lead to a massive explosion. West Pharmaceutical management had followed all the government guidelines for dust. In reality there are few dust regulations except for those governing the operations at grain silos. The rubber dust was a hidden danger just waiting to strike.[4]

No case may be stranger than the 2005 report of a fingertip in Wendy's chili. On March 22, 2005, Anna Ayala said she was eating chili at a Wendy's in San José, California. She felt something odd in her mouth and spit out a 1.5-inch fingertip. An investigation worthy of a *CSI* episode ensued. The fingertip was fingerprinted and DNA tested. All the workers from the restaurant were examined, and none were missing fingers. Similarly, no suppliers had employees report accidents with a lost finger. The finger was also evaluated to determine if it had been cooked or not. The finger was not cooked, indicating it was not part of the supply chain of ingredients for the chili. Wendy's first offered $50,000 then doubled the reward to $100,000 for information about the origin of the fingertip. Wendy's restaurants in northern California saw a major drop in business. Some employees were laid off, and some locations lost hundreds of thousands of dollars in business.

You probably know the rest of the story. Ayala herself had placed the fingertip in the chili. The fingertip was lost in a work-related accident by a friend of her husband. Wendy's management was

thrilled when an arrest was made.[5] But the financial and reputational damage had been done. You've probably heard one or more Wendy's fingertip jokes. The lost revenues were no joke. A piece of finger coupled with greed created a major crisis for Wendy's.

Crises happen more frequently than we might think. Every day there are product recalls and industrial accidents. Product tampering and management misconduct are not uncommon. The point is that companies are vulnerable to a wide array of threats or potential crises. Management cannot afford to say, "That could never happen here." If you sell food, some day it might be contaminated through tampering or by accident. If you have a production facility, it could be the site of a horrific industrial accident. Any company can have management that misbehaves. Companies must be prepared for crisis. We call that preparation crisis management.

CRISIS MANAGEMENT: THE REAL PREPARATION

There are two basic objectives to crisis management: (1) prevent a crisis from occurring and (2) lessen the damage from a crisis if one does happen. Experts argue that all crises have warning signs.[6] A few minor accidents indicate that a major one could occur. Improper quality control checks could result in harmful products going to market. There were a series of small accidents at the Union Carbide facility in Bhopal prior to the worst industrial accident the world ever witnessed in 1984. Crisis managers work to find the warning signs and prevent the crisis. The problem is recognizing the warning signs. Sometimes it is hard to tell a signal is a warning sign until it is too late and the crisis erupts. As the saying goes, "Hindsight is 20/20." It is much easier to see the warning signs after a crisis than before. After a crisis, you know where an event is leading, but that may not be clear before the crisis. Before the crisis you have to project where an event might go. In emergency management, efforts to prevent crises are referred to as *mitigation*. Mitigation identifies and reduces risks.

Regardless of your best efforts to prevent crises, a few will sneak by. That is why crisis management also seeks to reduce the damage from the crisis. Crisis managers try to prevent injuries, deaths, financial loss, property damage, environmental damage, and reputational damage. Crisis managers seek to protect stakeholders, the organization, and the industry. Effective crisis management can

reduce the physical and financial harms stakeholders face in a crisis. For example, swift and effective evacuations following a chemical release can protect the lives and health of community members. Organizations need to protect physical, financial, and reputational assets during a crisis.

A crisis in one corporation can threaten an entire industry. An *E. coli* outbreak in Odwalla juices is an example. Odwalla is one of a handful of juice makers that did not pasteurize their juices. Their natural processes seek to retain the fruits' and vegetables' original nutrients. These companies have strict policies about their raw materials to safeguard against *E. coli* and other contaminants. The Odwalla crisis raised fears that not pasteurizing might be too dangerous. Odwalla shifted to a flash pasteurization process. If the government concluded all juice should be pasteurized, the non-pasteurized juice industry would be no more. The Food and Drug Administration (FDA) does not require juices to be pasteurized but warns people of the risk of exposure to the bacteria when they drink them.

Crisis management is "a set of factors designed to combat crises and to lessen the actual damage inflicted by a crisis."[7] Thinking of crisis management as a set of factors is at the heart of viewing crisis management as company DNA. Too many crisis managers think that simply having a crisis management plan is crisis management. Too often preparation is assessed by the question, "Do you have a crisis management plan?" A plan in a binder is not crisis management. A crisis management plan is not equivalent to being prepared. The crisis plan does nothing to help your organization combat crises on a day-to-day basis. A crisis management plan (CMP) in a binder is an add-on, something you have. Some companies may go a step further and perform media training, in which members of the organization are trained to handle media questions in crisis situations.

A CMP and media training are valuable. However, they are not ends, they are means to an end. The end is true prevention and preparation, crisis management as DNA. CMP and media training are merely steps in preparation. A CMP is simply a reference tool in a crisis, not a how-to guide. And a crisis team that believes a CMP tells them the exact steps to follow in a crisis is in for a rude awakening and their stakeholders are in for a rough ride. A CMP preassigns tasks and responsibilities, provides important contact information, and contains forms to help crisis team members record

important information, such as stakeholder queries and what actions they have taken.[8] Media training may help your spokespeople deliver the crisis information and messages more effectively, but it does not collect the information or draft the messages to be sent. Neither a CMP nor media training contributes to mitigation. The best-managed crisis is the one that was avoided. CMPs and media training are like security blankets. Management feels better that they are there. But in reality, neither is sufficient to create effective crisis management.

To appreciate crisis management as DNA, it is helpful to consider the roots of crisis management. Crisis management evolved from emergency preparedness. Visit the Federal Emergency Management Agency (FEMA) Web site (www.fema.gov) and you will notice the similarities. FEMA requires all local areas to have emergency management plans. But FEMA does not equate a plan with preparation. Local emergency managers are required to regularly practice/exercise their plans. The type of exercise varies from sitting around the table discussing the crisis to in-the-field simulations with real people. Chapter 6 discusses the various exercise types. FEMA has a schedule for how often the various types of exercises should be performed. In addition, FEMA has local emergency managers engage in mitigation, their term for prevention. FEMA realizes that prevention is preferable to managing an emergency and that a plan is pointless unless it is tested through exercises. Hurricane Katrina highlighted the fact that FEMA, with its emphasis on preparation, can fail. No process is perfect in a crisis.

Crisis management as company DNA requires an ongoing commitment and execution of crisis management. Every organization needs a full-time crisis manager whose responsibilities include regularly collecting and assessing information about organizational risks. The crisis manager is trying to identify and then reduce crisis risks. The crisis manager is also responsible for keeping the CMP up to date and making sure there are regular crisis exercises. A CMP loses relevance as it sits on a shelf, because an organization evolves and those changes need to be reflected in the plan. For instance, the fact that people change jobs means that contacts and contact information changes. A CMP has no value until it is tested in an exercise. Only an exercise will help you determine if the CMP has the necessary and correct information and if the right people are on the crisis team.

OVERVIEW OF THE BOOK

Chapters 2, 3, and 4 identify the main types of crises organizations are likely to face. Cases are used to demonstrate the threat posed by the crises, identify ideas for detection and prevention, and illustrate effective and ineffective crisis responses. Each of these chapters provides a summary of what can be learned from the cases with a focus on the crisis response.

Chapter 5 is dedicated to the idea of a crisis-sensing network. The value of such a network is explained along with recommendations for creating one in your own organization. Chapter 6 returns to the idea of the CMP. The focus is on making the CMP a living document. The chapter also explains the value and variety in crisis exercises. Chapter 7 reviews the meaning of crisis management as organizational DNA. Recommendations are provided for how to move an organization from crisis management as an add-on to crisis management as DNA. The focus is on managing the organizational change necessary to make crisis management part of the organization's DNA.

I have tried to keep the book as jargon-free as possible. However, there is a language of crisis management. Table 1.1 provides a list of key crisis management terms and their definitions.

SUMMARY

In some ways, crisis management as an add-on may be more dangerous than no crisis preparation at all. If management thinks a CMP will protect them from harm, they are mistaken. CMPs do not actively seek to prevent crises, they help orchestrate responses to a crisis. If the plan is not updated or practiced, the crisis response will be ineffective and could even worsen the damage from the crisis. Crisis management as add-on creates a false sense of security that could lead to an ineffective or harmful crisis response.

Crisis management as DNA requires a true commitment. Top management must provide the resources and public commitment to crisis management. A crisis manager must routinely collect information that might contain risk information—engage in crisis sensing. Other departments in the organization need to respect and support the crisis management function by supplying the requested

TABLE 1.1:
KEY CRISIS MANAGEMENT TERMS

Accident Crisis: crisis that occurs because of technical-errors. The organization did not intend for the event to happen and/or could not control the event. The accident crisis category includes product harm, industrial accidents, transportation mishaps, challenges, and loss of key personnel.

Attack on Organization Crisis: crisis that occurs when some outside stakeholder or employee seeks to harm the organization in some way. The attack on organization crisis type includes product tampering, terrorism, rumors, workplace violence, and computer attacks.

Crisis: an unpredictable, major threat that can have a negative effect on the organization, industry, or stakeholders if handled improperly.

Crisis Management: a set of factors used to combat crises and to reduce the actual damage inflicted by a crisis.

Crisis Management Plan (CMP): a set of loose guidelines and forms that are used as a reference by the crisis team. It is sometimes called a crisis communication plan.

Crisis Management Team/Crisis Team: the people responsible for running crisis management effort and making key decisions.

Crisis Sensing Network: a mechanism for collecting and analyzing information about crisis risks. It is designed to funnel all possible crisis risk-related information to the crisis manager.

Crisis Types: the various categories of crises. Crises can be grouped into three types: attack on the organization, accident, and management misconduct.

Drill: an exercise that focuses on one element of crisis preparedness such as evacuation.

EOP: Emergency Operations Plan, a community plan for disasters that is similar to a CMP.

Exercise: a practice activity where people address a simulated crisis event.

Facilitator: a person who helps to develop, conduct, and evaluate a crisis exercise.

Federal Emergency Management Agency (FEMA): charged with preparing the U.S. for disasters and managing the federal response to disasters and recovery efforts. It is now part of the Department of Homeland Security.

Functional Exercise: an exercise that uses the Crisis Control Center and simulates interaction with emergency responders and other outsiders involved in the crisis. Does not involve the movement of real equipment or actions taken in the field.

Full-Scale Exercise: the most elaborate exercise where real actions are taken and the crisis team interacts with actual emergency responders and simulated crisis victims.

Incident: an occurrence of a crisis. Incident Management is often used synonymously with Crisis Management.

Instructing Information: information stakeholders need to know to protect themselves physically from a crisis such as shelter-in-place.

Hazmat: short hand for hazardous materials.

Management Misconduct Crisis: crisis created by management knowingly placing stakeholders at risk or purposefully violating laws or regulations. The management misconduct crisis type includes known risk, improper job performance, and purposeful legal/regulatory violation.

Mitigation: refers to efforts to prevent a crisis from occurring.

National Incident Management System (NIMS): the federal standard for the incident command structure to be used during disasters and crises. The idea is that all agencies will integrate more effectively if they all share an incident command structure. The use of NIMS is mandated by the Department of Homeland Security.

Orientation Seminar: an exercise where crisis team members learn about the CMP, their roles, and their responsibilities in a crisis.

Shelter-in-Place: when people are asked to stay inside and seal a building from outside air.

Stakeholder: anyone with an interest, or "stake," in the organization; stakeholder groups include employees and their families, customers, shareholders, directors, financial institutions, suppliers, distributors, government institutions (federal, state, and local), the media, and the communities in which an organization conducts business.

Tabletop Exercise: an exercise where members of the crisis team talk through a crisis situation.

information. The crisis manager also keeps the CMP current and makes sure there are regular drills to test the plan and the organization's level of preparedness. To maximize effectiveness, crisis management needs to be a part of your organization, embedded in the organization's DNA.

I

TYPES OF CRISES

2

Attacks on Organizations

In early 2005, there were high-profile security breaches at ChoicePoint and George Washington University. At ChoicePoint, the personal information of over 145,000 people in the United States might have been compromised. Hackers harvested 30,000 names, Social Security numbers, and other data from the student and faculty files at George Washington University.[1] The reality is that most attacks on corporate computer systems are performed by disgruntled employees, not outside hackers. Organizations are targets for attacks, both internal and external, in cyberspace and physical space. Attacks are premeditated actions designed to harm the organization and/or its personnel. Attacks also create collateral damage for stakeholders. Just ask the people whose identity information was lost at ChoicePoint and George Washington University if they are worried about identity theft.

Attacks on organizations take a variety of forms. All harm an organization reputationally and financially. The worst attacks result in loss of life of employees and/or external stakeholders. Product tampering, workplace violence, and terrorism fall on the extreme side because there is potential for loss of life. Computer hacking/tampering and rumors are less extreme but can be costly for

an organization and its stakeholders. Attacks are intentional actions taken by people working against the organization. There is no perfect defense against any of these attacks. All organizations are vulnerable in some fashion.

COMPUTER HACKING/TAMPERING

In today's wired world, computers and the Internet are indispensable. They are also a significant source of vulnerability. Outsiders can hack into a system or shut a system down through denial of service. Insiders can damage a system as well. Let's consider some examples of the different variations of computer hacking/tampering.

Online companies such as Amazon.com and eBay live by Internet sales. Yahoo! makes money by people visiting its Web sites. What happens when customers cannot access their Web sites? Lost customers equals lost revenue. Hackers use a procedure called denial of service to block access to Web sites. This causes the Web site to be overloaded with traffic, so there is no hacking. Routers are overloaded with so much fake traffic that real customers cannot access the site. Denial of service attacks require very little computer skills. Ironically, you can download programs for denial of service attacks from the Internet.[2] A set of attacks in February 2000 resulted in a estimated $100 million in lost revenues for various Internet companies. Among those affected were eBay for ninety minutes, Amazon for one hour, Yahoo! for three hours, and e-Trade for ninety minutes. The source of the attack? A fifteen-year-old Canadian hacker.[3] Denial of service is a federal crime in the United States. The FBI handled the 2000 cases. Denial of service can cost organizations and investors money.

Computer Hacking Case: ChoicePoint

ChoicePoint is a data brokering firm. Their databases include Social Security numbers, credit and medical histories, motor vehicle registration, job applications, lawsuits, criminal files, and other sensitive information. The database has over 19 billion entries. The thieves created false accounts by posing as clients of ChoicePoint. It is known that 35,000 people had their detailed information taken.

A total of 110,000 people were sent letters warning them that their information may have been compromised. Police only learned about the case because California law requires a company to notify people about security breaches that could compromise their identities. Very few states have such notification laws. Authorities estimate that up to 500,000 people could be at risk. The thieves used fax machines at a Kinko's office to run the scam. One arrest has been made so far.[4] In 2004, hackers breached a computer at the University of California at Berkeley and harvested information from 1.4 million personnel records of state in-home care receivers.[5] Hacking can place customers at risk for identity theft.

Hacking/tampering can be a result of insider attacks. A study sponsored by the U.S. Department of Homeland Security found that most insider attacks are committed by employees seeking revenge against their bosses. Employees might be angry over a disciplinary action, missed promotion, or a layoff, for example. In one case an employee unhappy with his severance package caused a company's communication system to go down for two days. In addition to crippling networks, insider attacks might delete critical software. Whatever the nature of the attack, the organization takes a financial loss.[6]

But should we really worry about computer hacking/tampering? Yes. Studies show that about 90 percent of all corporations detected at least one computer security breach per year. The FBI estimates that only about 34 percent of such crimes are ever reported. Corporations fear the negative publicity.[7] Your company and your stakeholders are at risk.

Prevention and Detection

The Pentagon contends with hundreds of computer attacks each day. The good news is they have a high success rate in defeating the attacks. The bad news is that your organization is probably not the Pentagon. You probably have some sort of firewall to protect your computer. Though that is good, it is not enough to protect your organization. Security experts recommend a range of intrusion detection devices and software and even countermeasures. The devices and software warn an organization of an attack, an attempt to breach security, or a denial of service. There are aggressive programs that respond in kind to denial of service attacks. Your company needs to decide what is right for its goals.

There are two steps that are critical to prevention of computer hacking/tampering. The first is a thorough analysis of your computer-based vulnerabilities. Where are you vulnerable? What types of equipment, software, security, protocols, and training can help address those vulnerabilities? Internal threats are best prevented through proper security clearance, including biometrics, and encryption. A worker who has been laid off should not be able to reenter the facility or the computer system. Experts note that there are warning signs for inside saboteurs. The warning signs include tardiness, missing work, and arguing with co-workers. Management should monitor employees facing disciplinary action and provide formal grievance procedures for those who feel wronged.[8] Make sure only the authorized personnel have complete access and the ability to revoke access if an employee appears to be a problem. Also, it is important to train people so they know the proper security protocols and do not accidentally give vital information away or allow people into your system by loaning them their computer ID.

Basic Crisis Response

The response to computer hacking/tampering is delicate. Why announce a problem when you don't have to? That logic has limited applications. First, other states are following California's lead and requiring companies to contact stakeholders when their identity information may have been compromised. It takes an average of three years to recover from identity theft.[9] It is good customer service to warn the people that they have been placed at risk. It is also the basic crisis response. Your first message should tell people what to do to protect themselves from the crisis. If stakeholder identities are at risk, send them a letter of notification that includes the steps they should take. Second, the FBI has special InfraGard chapters that keep investigations private. The news media will not find and publish a police report. The FBI can help your organization fix the problem without publicity.

If the crime goes public, explain what preventive measures were in place prior to the incident, note what is being done to solve the crime, and indicate general changes designed to prevent a repeat of the crisis. You may or may not want to talk about future preventive actions. Security is best kept private so you can just note that changes will be made without providing details. Remember that your company is a victim, too. It's all right to acknowledge that.

RUMORS

Rumors are untrue information about your organization that are circulating publicly. The key points here are *untrue* and *public*. Bad news about your company that is true is not a rumor. Someone expressing a negative opinion about your organization, product, or service is not a rumor. The Internet has facilitated the ability to spread rumors. With millions of people posting and e-mailing millions of messages each day, cyberspace is fertile ground for rumors. Visit either www.snopes.com or www.truthorfiction.com to separate Internet fact from fiction. Both sites are dedicated to debunking rumors.

Rumor Case: The Infamous Tommy Hilfiger Comment

In 1996, the Internet was abuzz with the Oprah–Tommy Hilfiger showdown. Messages about the conflict were sent via e-mail and posted at various discussion groups. A sample message is provided in Exhibit 2.1. The basic story is that clothing designer Tommy Hilfiger appeared as a guest on the *Oprah Winfrey Show*. She asked him if it was true that he did not like having African Americans, Hispanics, and Asians wearing his clothes. He said "yes" and that he wished those people would not wear his clothes because they were not made for them. Oprah then threw him off of her show.

Exhibit 2.1

Subject: FWD: Tommy Hilfiger hates us . . .

Did you see the recent Oprah Winfrey show on which Tommy Hilfiger was a guest? Oprah asked Hilfiger if his alleged statements about people of color were true—he's been accused of saying things such as "If I had known that African-Americans, Hispanics and Asians would buy my clothes, I would not have made them so nice," and "I wish those people would not buy my clothes—they were made for upper-class whites." What did he say when Oprah asked him if he said these things? He said "Yes." Oprah immediately asked Hilfiger to leave her show.

Now, let's give Hilfiger what he's asked for—let's not buy his clothes. Boycott! Please—pass this message along.

Tommy Hilfiger has never appeared on the *Oprah Winfrey Show,* nor has he ever made such statements. In fact, Hilfiger ads feature a

diverse group of models. The rumor was untrue, but the e-mails and the postings calling for boycotts (the threat) were real. Hilfiger could have lost customers because of the rumor and did suffer reputational damage. Who wants to be known as a racist? The company used the Internet to respond to the rumor. Responses from the company were posted at discussion groups where the rumor was being talked about. A section of the company's own Web site was dedicated to the rumor, www.tommy.com/about/about_us.aspy?cat=Rumor. Exhibit 2.2 lists comments from the site, including one from Tommy Hilfiger and one from Oprah Winfrey. You can also find refutations at the two rumor debunking sites noted earlier.

Exhibit 2.2

Tommy Hilfiger: "I am deeply upset that a malicious and completely false rumor continues to circulate about me. I create my clothing for all different types of people regardless of their race, religious or cultural background. I want you to know the facts so that you are not the victim of a classic 'urban myth' that perpetuates untruths and has no basis in reality. Please read further to learn the truth."

Oprah Winfrey: "So I want to just set the record straight once and for all. The rumor claims that clothing designer Tommy Hilfiger came on this show and made racist remarks, and that I then kicked him out. I just want to say that is not true because it just never happened.

"Tommy Hilfiger has never appeared on this show. READ MY LIPS, TOMMY HILFIGER HAS NEVER APPEARED ON THIS SHOW. And all of [the] people who claim that they saw it, they heard it—it never happened. I've never even met Tommy Hilfiger."

Taped live on *The Oprah Winfrey Show*, January 11, 1999

The rumor originated in a Philippines tabloid newspaper. The original story claimed Hilfiger had said he had not made the clothes for Filipinos and wished they would stop wearing them. A variation has the incident occurring on *CNN Style* with designer Elsa Klensch. A nearly identical rumor spread about Liz Claiborne in 1991.

But these are rumors, right? "Sticks and stones will break my bones but words will never hurt me." Experts disagree. Don Middleberg, a pioneer in cyber–public relations, observes, "A lot of stuff [statements in cyberspace] is malicious. If companies let these

rumors fester without responding to them, they can get hurt."[10] Rumors damage reputations and ultimately inflict financial damage if the reputation is damaged enough.

Prevention and Detection

Clearly we cannot prevent a rumor. People will create messages and place them in cyberspace. Other people will find the messages interesting and believable and relay them. That is human nature—rumors have spread for thousands of years without the Internet. In the 1980s, a popular rumor was that the candy Pop Rocks would explode in your stomach if you ate them and then drank a soda. Now it is easier to reach more people and faster. Prevention in this case means preventing or limiting damage and that is keyed to detection.

Detection involves a close monitoring of the Internet. Easier said then done, you might protest. The Internet is composed of millions of Web pages, discussion postings, and web logs or blogs. The good news and bad news is that these messages are public. You can find them, but so can your stakeholders. Companies such as CyberAlert (www.cyberalert.com) and eWatch (www.ewatch.com), specialize in monitoring all facets of the Internet for statements about your organization. For a fee, they will monitor, collect, and analyze Internet comments about your organization. They will perform the standard searches of the Internet news media as well as print, radio, and television. By casting a wide net you can identify rumors early.

Basic Crisis Response

The old logic for rumors was to ignore them and they would fade away. As Middleberg suggests, the best response now is take the offensive. Messages have a long life and potential reach on the Internet. The response to a rumor should follow the two-pronged approach of Tommy Hilfiger. First, post replies to sites on the Internet where the rumors are found. Make it clear you represent the organization in question. Provide evidence to support your claim and links to additional sites for further information. Second, dedicate part of your Web site to refuting the rumor. Provide evidence, including testimonials, that debunk the rumor. Tommy Hilfiger's site included a testimonial from Oprah herself. You can even provide links to other sites that support you. The Hilfiger site featured links to the rumor on both the snopes.com and truthorfiction.com Web sites. When Febreze faced

@inproceedings{Coombs2006CodeRI, title={Code Red in the Boardroom: Crisis Management as Organizational DNA}, author={W. Timothy Coombs}, year={2006} }. W. Timothy Coombs.Â Organizational Crisis Communication Translated in the Networked Society. Heather C McIntosh. 2018. Measuring the crisis preparedness in the pharmaceutical sector: the case of greece. Laura Maska, Theodore Tsekeris, Christos Kadas, Charalambos Tsekeris. 2017. Code Red in the Boardroom: Crisis Management as Organizational DNA. Westport, CT: Praeger; Coombs, W. (2007). Ongoing Crisis Communication: Planning, Managing, and Responding (2nd ed.).Â The landscape survey looks for clues in the organizationâ€™s internal and external environments that may indicate the presence of an unethical event brewing. Potential crisis indicators include the ethical environment of the Board of Directors, the safety policies of the organization, the economic motives among top executives and management, the degree of industry vulnerability, and the vulnerability of the organization in the global environment. These indicators are discussed next. Code red in the boardroom: Crisis management as organizational DNA. Westport, CT: Praeger. Analysis of Pakistan print media narrative on the war on terror.Â An organization's image and reputation are assets that are built up over time. Organizations seek to develop and maintain positive images in the minds of publics. The image of an organization can be threatened by crises, and this impacts the trust it has with its employees and customers. Trust declines when employees feel they are not informed properly, especially in times of crises when it is imperative to respond to the threat and where promptness is necessary. Communications help build or restore some level of trust.