

# **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.

Copyright © 2006 by W. Timothy Coombs

All rights reserved. No portion of this book may be  
reproduced, by any process or technique, without the  
express written consent of the publisher.

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* ix

1. Introduction: Crises Do Happen, So Be Prepared 1

## I TYPES OF CRISES

2. Attacks on Organizations 13

3. When Things Go Bad 27

4. When the Organization Misbehaves 45

## II CRISIS MANAGEMENT

5. Crisis-Sensing Network 65

6. The Crisis Management Plan as  
Living Document 77

7. Crisis Management as DNA: Overcoming  
Resistance to the Crisis Management Process 91



<i>Appendix A: Sample Crisis Management Plan Elements</i>	103
<i>Appendix B: Department of Homeland Security Fact Sheet for NIMS</i>	111
<i>Notes</i>	115
<i>References</i>	125
<i>Index</i>	133

---

# 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 versus 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.<sup>1</sup>

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.<sup>2</sup> 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.<sup>3</sup> 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.<sup>4</sup>

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.<sup>5</sup> 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.<sup>6</sup> 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."<sup>7</sup> 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