Chapter 4.15
Crisis Compliance:
Using Information Technology to Predict, Prevent and Prevail over Disasters

Laura Lally
Hofstra University, USA

ABSTRACT

This article develops the concept of crisis compliance (CC)—defined as making appropriate use of IT, and non-IT methodologies to predict, prevent, and prevail over disasters. CC emerges from Lally's Target Shield and Weapon Model, which is grounded in the theories of crisis management, normal accident theory, and high reliability organizations. CC is then applied to a case study involving Hurricane Katrina, with examples drawn from other recent disasters. Emerging IT-based crisis management initiatives will be examined with an emphasis on how the impacts of Hurricane Katrina could have been mitigated. Recommendations for predicting, preventing, and prevailing over future disasters will emerge from the analysis.

INTRODUCTION: THE INCREASE IN CRISES AND IT-BASED INITIATIVES TO COMBAT THEM

The post 9/11 environment has been characterized by an increasing number of crises. Crisis management researcher Ian Mitroff (2005, p. 3) notes:

The number of crises not only is growing rapidly, but of even greater concern, is the fact that the rate of increase in the number of crises is increasing as well. Furthermore the time, and even the geographical distance, between crises is shrinking precipitously.

There has been a corresponding increase in public awareness of the potential for crises, not only from terrorist attacks, but from accidental

failures such as blackouts and natural disasters such as hurricanes. The widespread traumatic impacts of crises such as 9/11, Hurricane Katrina, and the Sumatra-Andaman earthquake and resulting tsunamis, has lead to an increased emphasis on disaster planning on the part of national and local governments.

Government funding for new technologies aimed at combating terrorist attacks and other disasters has increased, and a wide range of new IT-based systems and methodologies have emerged. This article will argue that methodological breakthroughs and emerging technologies for combating disaster in one domain, such as battling terrorism, fighting natural disasters, or mitigating the impact of major accidents such as blackouts and hazardous material spills, can be applied to disasters in other domains as well.

IT can provide managers and government leaders with a means of: (1) educating their employees or citizens about the realistic likelihood of the occurrence of a potential disaster, (2) disseminating up-to-the-minute information about any disasters that are immediately threatening, (3) mitigating the impact of disasters through evacuation planning, healthcare availability, and emergency food and water supplies, and (4) recovering from the disaster and rebuilding.

This article develops the concept of crisis compliance (CC)—a framework for approaching crises that focuses on three questions: (1) What IT-based tools are available for *predicting* a crisis, *preventing* the effects from spreading, and *prevailing over* future crises? (2) What is the appropriate use of these technologies in a given crisis scenario?, and (3) What are the responsibilities and obligations of managers and government leaders to use these tools appropriately? The research will argue that if a manager or government leader has made full use of IT-based decision making and communication tools, as well as non-IT methodologies appropriate for a given crisis, the decision maker has been CC.

Mitroff (2005) indicates that, "One of the most striking and interesting feature of crises is that, virtually without exception, they are experienced as major acts of betrayal" (p. 39). He defines betrayal as:

Betrayal is the failure of a person, an organization, an institution, or a society to act and behave in accordance with ways that they have promised or they have lead us to believe they will. Betrayal is the violation of trust that we have placed in another person, organization, institution and/or society. Thus, betrayal is profoundly rooted in our basic feelings of trust and goodness with regard to others ....In every case, betrayal is the violation of a basic and fundamental assumption we are making about an individual, an organization, an institution or society—for example, that another person will stand up for us, act in our best interests, and protect us. When the assumption—or more commonly, a set of assumptions—has been showed to be false or invalid, as in Oklahoma City and 9/11, we are stunned. We are left with the feeling of having been betrayed to our core. (p. 40)

In August 2005, Hurricane Katrina hit the Gulf Coast of the United States, causing over 1,500 lives to be lost and irreparable damage to many homes, businesses, and unique historical landmarks. A devastating revelation in the aftermath of Hurricane Katrina was that many of the IT-based strategies that were available were not used, or were used and the results not acted upon. This raises the issue that the local, state, and federal governments did not respond as citizens of a highly technologically advanced society would have expected them to. These disastrous failures lead to widespread feelings of betrayal—feelings that the government and many local industries had failed in their moral obligations to citizens who were stakeholders in the communities that were affected.

Related Content

The Waterfall Approach and Requirement Uncertainty: An In-Depth Case Study of an Enterprise Systems Implementation at a Major Airline Company
Huub J.M. Ruël, Tanya Bondaroukand Stefan Smink (2012). *Project Management Techniques and Innovations in Information Technology (pp. 49-65).*
www.irma-international.org/chapter/waterfall-approach-requirement-uncertainty/64954

Cyberbullying: A Case Study at Robert J. Mitchell Junior/Senior High School
Michael J. Heymannand Heidi L. Schnackenberg (2011). *Journal of Cases on Information Technology (pp. 1-8).*
www.irma-international.org/article/cyberbullying-case-study-robert-mitchell/60382

The FBI Sentinel Project
Leah Olszewskiand Stephen C. Wingreen (2011). *Journal of Cases on Information Technology (pp. 84-102).*
www.irma-international.org/article/fbi-sentinel-project/56310

Effect of Tasks, Salaries, and Shocks on Job Satisfaction Among MIS Professionals
Fred Niedermanand Mary Sumner (2006). *Advanced Topics in Information Resources Management, Volume 5 (pp. 184-210).*
www.irma-international.org/chapter/effect-tasks-salaries-shocks-job/4648

Impact of Organisational Intranets on Profitability in Organisations
Udo Richard Averweg (2008). *Information Communication Technologies: Concepts, Methodologies, Tools, and Applications (pp. 2817-2844).*
www.irma-international.org/chapter/impact-organisational-intranets-profitability-organisations/22849