INFORMATION TECHNOLOGY AND CRISIS COMPLIANCE: IMPLICATIONS FOR STUDYING HURRICANE SANDY

Laura Lally
Department of IT/QM
Frank G. Zarb School of Business
Hofstra University
Hempstead, NY 11550
Laura.H.Lally@hofstra.edu
(516) 463-5351

ABSTRACT

This paper develops a comprehensive framework for the role of IT in Crisis Compliance—the use of IT to predict crises, prevent them from occurring, prevailing over the ones that do occur, and aiding in Post-Crisis Renewal. Theoretical perspectives from Crisis Management, Normal Accident Theory, High Reliability Organizations, and the Target and Shield Model will inform the analysis. Additional implications for characterizing whether IT is the cause, prevention, or cure of the crisis, applying the model to diverse urban areas, dealing with malevolent threats, distinguishing betweenprecedented and unprecedented threats, and determining the scope of the crisis will extend the theoretical framework. Suggestions for studying Hurricane Sandy in the light of this framework will conclude the analysis.

Keywords: Crisis Compliance, Crisis Management, Normal Accident Theory, High Reliability Organizations, Target and Shield Model, Hurricane Sandy, Post-Crisis Renewal.
INTRODUCTION: THE ROLE OF IT IN CRISES

Information Technology (IT) has created both the potential for threats that can lead to major crises, and opportunities for creating systems to help prevent crises, prevail over crises if they do occur, and aid in Post Crisis Renewal. This paper develops a theoretically based framework for educating individuals, organizations, and government leaders about how to approach IT based threats and opportunities.

The paper focuses on the topic of IT and Crisis Compliance (CC), developed by Lally [9,10]. Crisis Compliance is defined as: 1) the development of methodologies and systems to prepare individuals, organizations and government leaders to predict, prevent and prevail over crises, 2) the development of an awareness of IT based best practices currently available for combating crises, 3) the development of an understanding of newly emerging technologies, their vulnerabilities that could make them crisis prone as well as their potential for combating crises, 4) the development of an understanding of the obligation of individuals, managers and government leaders to make use of these technologies in an appropriate manner, and 5) the development of an understanding of how IT based systems aid in Post-Crisis Renewal (PRC)—the restoration of well being and culture in the wake of a crisis.

Crisis Compliance argues that if the proper methodologies are used, then individuals, organizations and governments will have fulfilled their obligations to their stakeholders and be free from unfair criticisms and potential lawsuits. Crises are resulting in an increasing number of lawsuits resulting in large financial settlements and even manslaughter convictions [1]. Crisis Compliance cannot guarantee that no crisis will arise and that no negative impacts will occur, but rather that organization and government leaders have done everything humanly possible to predict the crisis, prevent its occurrence and mitigate negative impacts, to create a learning environment to help prevail over future crises, and to help restore well being and culture after the crisis has passed. Crisis Compliance draws on the theoretical perspectives of Perrow’s Normal Accident Theory, the Theory of High Reliability Organizations and Lally’s IT Target and Shield Model.

NORMAL ACCIDENT THEORY (NAT) AND THE THEORY OF HIGH RELIABILITY ORGANIZATIONS (HRO)

The first theoretical perspective, which addresses the potential threats involved in large scale systems is Charles Perrow’s Normal Accident Theory. Normal Accident Theory (NAT) argues that characteristics of a system’s design make it more or less prone to accidents. Accidents are defined as [14] "a failure in a subsystem, or the system as a whole, that damages more than one unit and in doing so disrupts the ongoing or future output of the system." Perrow distinguishes between disastrous "accidents," which are system wide and seriously impact the system's overall functioning and "incidents," which involve single failures that can be contained within a limited area and which do not compromise the system's overall functioning. Perrow argues that no system can be designed to completely avoid incidents, but that inherent qualities of the system determine how far and how fast the damage will spread. Systems that are not designed to contain the
negative impact of incidents will, therefore, *be subject to accidents in the course of their normal functioning*.

The first key characteristic of accident prone systems is their complexity. **NAT** argues that as systems become more complex, they become more accident prone. **NAT** distinguishes a second characteristic of systems that exacerbate potential problems brought about as a result of complexity -- tight coupling. Tight coupling means there is no slack time or buffering of resources between tasks, interactions happen immediately. **NAT** distinguishes one further characteristic of disaster prone systems, a lack of control.

Researchers in High Reliability Organizations (**HRO**) have examined organizations in which complex, tightly coupled, technologically based systems appeared to be coping successfully with the potential for disaster. High reliability theorists’ studies of the Federal Aviation Administration's air traffic control system, the Pacific Gas and Electric's electric power system, including the Diablo Canyon nuclear power plant, and the peacetime flight operations of three United States Navy aircraft carriers indicate that organizations can achieve nearly error free operation [8].

**HRO** theorists identify four critical causal factors for achieving reliability:

* Political elites and organizational leaders put safety and reliability first as a goal.
* High levels of redundancy in personnel and technical safety measures.
* The development of a "high reliability culture" in decentralized and continually practiced operations, and
* Sophisticated forms of trial and error organizational learning.

The two theories have been contrasted as "pessimistic" -- **NATs** contention that disaster is inevitable in badly designed systems, versus "optimistic" – **HROs** pragmatic approach to achieving greater reliability. The theories, however, are in agreement as to which characteristics of systems make them more or less accident prone.

**LALLY’S TARGET AND SHIELD MODEL**

Lally [4] argued that Normal Accident Theory was a sound theoretical perspective for understanding the risks of Information Technology, because IT is complex, tightly coupled and often poorly controlled. She also argued [5] that IT based systems do not operate in isolation but in organizational settings where failures in IT can lead to more widespread secondary failures in organizations and to society as a whole. Additionally, she argued [6] that the frequent rapid change in both IT based systems and the work processes they support can further exacerbate the potential for disaster. These characteristics are what permitted a design flaw, such as Y2K, considered “trivial” by software designers to potentially propagate into a global disaster and why even the experts were unable to predict what the impact would be.

Figure 1 illustrates the Target and Shield Model
Lally [7] further extended her model and argued that IT based systems are not only a target used as a weapon of destruction to cause serious accidents, but that IT based systems can be a shield used to prevent damage from future incidents, whether they be IT based or physical.

The Target and Shield model incorporates Lally’s extensions to Normal Accident Theory. The model also contains three significant feedback loops, which allow IT to play a positive role in preventing future incidents from materializing, having real world impacts, and mitigating their impacts when they do occur. In the Feedback Loop #1, Prevent future incidents, controls can be built into the system to prevent future incidents from materializing. In Feedback Loop #2, Prevent Propagation of Incidents, controls can be built into the system to prevent future incidents that have materialized from turning into accidents. In the Feedback Loop #3, Mitigate Impact of Disasters, IT based systems can be developed to prevent accidents resulting from IT based or physical attacks from propagating even further, and to provide more rapid recovery and renewal of culture and quality of life.

TECHNOLOGY—SOURCE OF THE CRISIS, PREVENTION, CURE?

An important characteristic of a crisis when examining the role of IT is whether the crisis is technology based. Y2K clearly had its foundation in poor software design and the rapid expansion and proliferation of technology. Hurricane Katrina, however, was a natural disaster in which IT could have played a much more successful role in combating the crisis than it did. When organizations use white hat hackers or war gaming experts to simulate cyberattacks with the goal of preventing future attacks [2], IT is used as both a target and shield.

EXTENDING THE MODEL TO CRISES IN DIVERSE AREAS

An additional factor that emerged in the Post 9/11 environment was that disasters can occur in large scale social environments such as cities and nations, rather than in organizations. NAT and HRO, which were developed to prevent innocent mistakes from propagating into system-wide disasters in organizational settings had to be extended. Lally [8] addressed challenges of extending the models to large diverse environments, rather than organizational settings. Large areas add additional layers of complexity and tight coupling when compared to organizational settings.

UNPRECEDENTED CRISES POSE GREATER CHALLENGES

Another characteristic of crises that add to the potential for damage is whether or not they are unprecedented. Both Y2K and 9/11 had no precedent on the scale at which they occurred. Despite 130 years of technological advances, civil reform, and building code updates, Japan’s 2011 earthquake and tsunami resulted in 20,000 deaths [3]. In these cases there was no collection of best practices to draw on.
THE CHALLENGE OF MALEVOLENT THREATS

A final characteristic of crises is whether or not they are the result of malevolent actions. Y2K was caused by an inadvertent error by program designers. The result of extensive Y2K testing has lead to better software design. 9/11, however, was malevolent and preventing the reoccurrence of another major terrorist attack involves investigating groups of individuals who may or may not be guilty with serious implications for privacy and civil rights.

CRISIS AND SCOPE

Another characteristic of crises is their scope. Can the crises be controlled by quarantining the area or will the effects of the crisis spread quickly? Sites like Chernobyl were remote and able to be quarantined, resulting in limited impact outside the effected area. The March, 2011 tsunami and nuclear disaster in Japan posed serious threats to the people of Tokyo, and resulted in nuclear radiation increases in California.

CRISIS COMPLIANCE AND THE SEARCH FOR FEASIBLE SOLUTIONS

When implementing IT based systems in a crisis situation the issue of feasibility must be addressed. Four essential types of feasibility emerge:

Technical feasibility—Is there an IT based solution to the problem? Solutions that required cell phones, the Internet and digital cameras would be feasible now but not forty years ago. For organizations to be Crisis Compliant, their disaster plans need to include the most recent technology.

Operational feasibility—Will the solution work in the given environment? Technically sophisticated users will more readily adopt new technologies. Technologies are more likely to be adopted in High Reliability Organizations with strong organizational cultures that support its use.

Economic feasibility—Can we afford the solution (or afford not to use it)? The high risk exposure to hurricanes in New Orleans was well known but budgetary constraints prevented the development of stronger levees. Flood protection in the Netherlands far surpasses what was and is currently available on the Gulf Coast because the government placed a high priority of protecting its citizens.

Schedule feasibility—Do we have time to implement the solution? In unprecedented crises, such as 9/11, leaders did not have adequate lead time to envision the full extent of the problem and respond with optimal solutions. Government leaders could argue that schedule feasibility did not permit full compliance. In the case of Katrina, however, there had been years of warnings and a simulation model the year before indicated results very similar to those which actually happened, yet the problem was not responded to.
Electricity and information are the twin life bloods of modern societies. If electricity and information are disrupted, then everything from the production of food to the supply of potable water, to ATM service service—literally everything in modern society—grinds to a halt—We are truly coupled and interdependent as never before. [12, p. 13].

Hurricane Sandy was a natural disaster on a scale that was unprecedented in recent history. The storm was predicted several days in advance allowing for mass evacuations and a relatively low loss of life, compared to hurricanes like Katrina. Major property damage did occur in many waterfront communities including Breezy Point Queens, the New Jersey Shore, and Coney Island. Many historical landmarks on the waterfront were destroyed by the nine foot storm surge. Flooding caused extensive power blackouts that included lost heat and water, including Manhattan below 34th Street for a week, and areas of Long Island, Staten Island and New Jersey for up to two weeks, leaving individuals unable to obtain information through television or the Internet. The storm caused major disruptions in transportation—the Midtown and Brooklyn Battery Tunnel were closed for over a week, and gas shortages prevented the use of automobiles.

A number of questions emerge in the light of the theoretical analysis.

1. Was Sandy truly unprecedented, especially in the light of Hurricane Irene the year before?
2. What technically feasible solutions, such as those used by the Netherlands, London, and Hong Kong, could have mitigated the damage?
3. What were the responsibilities of governments, utilities, and individuals living in red zones? How well were these responsibilities fulfilled?
4. How did the initial damage of the storm (high winds and storm surge) propagate into secondary damages (gas shortages, long term power outages, business losses, unemployment)? How could this propagation have been minimized?
5. How can the culture of the neighborhoods affected, and the New York Metropolitan Area aid in Post-Crisis renewal?

The focus of upcoming case study will be to highlight in depth the nature of the disaster in the context of Crises Compliance, and to suggest IT and non-IT solutions and methodologies to predict, prevent, and prevail over future hurricanes.

REFERENCES


*This research was supported by a Summer Grant from the Frank G. Zarb School of Business*
Figure 1: The Target and Shield Model

**Target**

- **Control: Intercept**
  - Potential Incidents
  - Complexity (+)
  - Tight Coupling (+)
  - Change (+)
  - Real World Impacts
- **Control: Mitigation**
  - Complexity (+)
  - Tight Coupling (+)
  - Change (+)
  - Secondary Impacts

**Shield**

- **Prevent future incidents**
  - Loop #1
- **Prevent propagation of incidents**
  - Loop #2
- **Mitigate Impacts of Disasters**
  - Loop #3