Journal of International Business and Law

Volume 16 | Issue 1 Article 6

5-1-2016

# Crisis Compliance for International Technology Based Risks: Lessons from Fukushima

Laura Lally

Brian Garbushian

# CRISIS COMPLIANCE FOR INTERNATIONAL TECHNOLOGY BASED RISKS:

# LESSONS FROM FUKUSHIMA

*By Laura Lally[*] and Brian Garbushian[**]*


## ABSTRACT

International Organizations require guidelines for dealing with Technology Based Risk. This paper presents a framework for the role of technology in crises—Crisis Compliance—the use of technology to predict crises, to prevent them from occurring, and to prevail over the ones that do occur and extends it to international organizations and industries. This framework is applied to the disaster at Fukushima and it explores the Japanese government's role in deploying nuclear technology, responding to the immediate crisis, and coordinating the massive ongoing cleanup effort. Five characteristics of the crisis emerge: 1) "Design Basis" versus "Beyond Design Basis" Risks—what risks are "built-in" to nuclear technologies versus those that are "outside the box," 2) Deterministic versus Stochastic Risks—risks whose impact is immediately visible versus those risks whose effect are only visible long term, 3) Physical and Geographical Scope—the degree to which the risk can be physically isolated, 4) Contained versus Cascading Disasters—disasters of one particular type versus those that evolve into other forms of disasters, and 5) Internal versus External Locus of Control— industry's ability to regulate itself versus the need for independent regulatory agencies. Application of this framework to other technology based crises provides further examples of how an understanding of these characteristics can provide insight into dealing with international Technology Based Risk in the future.


**Keywords:** Crisis Compliance, Crisis Management, Technology Based Risk, Fukushima, High Reliability Organizations, Normal Accident Theory, Target and Shield Model.

## Crisis Compliance and Fukushima

International organizations require guidelines for dealing with Technology Based Risk. This paper presents a theoretically based framework--Crisis Compliance--for educating individuals, organizations, and government leaders on how to approach a crisis and on how to apply it to international organizations and industries. Crisis Compliance is defined as: 1) the

[*]Associate Professor Department of Information Systems and Business Analytics Frank G. Zarb School of Business at Hofstra University.
[**] Financial Planning and Analysis at AECOM, New York, NY.

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 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, and 4) the development of an understanding of the *obligation* of individuals, managers and government leaders to make use of these best practices and technologies in an appropriate manner.

Crisis Compliance argues that if appropriate technologies are used and best practices are followed, then individuals, organizations and governments will have fulfilled their obligations to their stakeholders and will 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 (Mitroff, 2005), (Lash & Wellington, 2007), (Associated Press, 2012). Crisis Compliance neither guarantee that a crisis not will arise, nor and that no negative impacts will not occur. Rather, it guarantees that organization and government leaders have done everything humanly possible to predict the crisis, to prevent its occurrence/mitigate negative impacts, to create a learning environment that will help prevail over future crises, and to help restore the sense of well-being and the 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 Target and Shield Model. A case study of Fukushima will first place the disaster in the context of Crisis Compliance. The study will then expand and extend the concept of Crisis Compliance and examine the implications of these extensions for the future of the international nuclear industry.

This study will address the following questions: 1) Was technology used appropriately to prevent the Fukushima disaster? 2) Was technology used appropriately to mitigate the damage? and 3) How can technology be used to prevent future disasters, help in disaster recover, and help in the post-crisis renewal?

## Frameworks for Studying Crises

Three theoretical frameworks provide a basis for international Crisis Compliance: 1) Perrow's Normal Accident Theory, 2) the Theory of High Reliability Organizations and 3) Lally's Target and Shield Model.

## Normal Accident Theory (NAT)

The first theoretical perspective, which addresses the potential threats involved in large scale systems is Charles Perrow's Normal Accident Theory (1984, 1999). Normal Accident Theory **(NAT)** argues that the characteristics of a system's design make it more or less prone to accidents. 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. Perrow also notes that the greatest source of complexity is often the external environment and that having a system interact with the external environment is likely to cause a significant increase its complexity. Perrow also identifies "common mode failures" in which a single incident can cause multiple failures and notes these types of failures are a common source of accidents in complex systems.

Sargut and McGrath (2011) further distinguish between *complicated* systems, those that have many parts which move in predictable ways, and *complex* systems, those with many parts that move in ways that are continually changing:

> "Three properties determine the complexity of an environment. The first *multiplicity* refers to the number of potentially interacting elements. The second *interdependence* refers to how interconnected those elements are. The third *diversity* has to do with their degree of heterogeneity. The greater the multiplicity, interdependence, and diversity, the greater the complexity" (p 70).

**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, and interactions happen immediately. Tight coupling, like complexity, is often more efficient from a productivity standpoint. However, incidents tend to propagate faster and their impact becomes more severe because there is no lag time during which human intervention can occur and no buffer stocks to mitigate the impact of downtime.

**NAT** distinguishes one further characteristic of disaster prone systems, a lack of control. Tightly coupled, complex systems are difficult to understand, making potential problems harder to predict. Controls that would sense problems and respond to them need to be built into systems as they are developed, but rarely are due to economic and time constraints.

Perrow developed his theory while studying complex technologies such as nuclear power plants, like Three Mile Island and Chernobyl, where major disasters had happened, consequently determining the conditions under which incidents such as valve failures could lead to accidents such as nuclear meltdowns. **NAT** argues that human and technology based incidents need to be anticipated and controls need to be built into the system to prevent them and contain their propagation. The question as to whether nuclear power plants can be designed to prevent future disasters, or whether their inherent characteristics make them disaster prone, emerges from Perrow's work.

### The Theory of High Reliability Organizations (HRO)

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, and the peacetime flight operations of three United States Navy aircraft carriers, indicate that organizations can achieve nearly error free operation (Roberts, 1989), (La Porte & Consolini, 1991), (Sagan, 1993). (Klein, Bigely and Roberts, 1995), (Grabowski and Roberts, 1997).

**HRO** theorists identify three critical causal factors for achieving reliability: 1) political elites and organizational leaders put safety and reliability first, 2) the organization has high levels of redundancy in personnel and technical safety measures, 3) the organization has a high reliability culture, that involves sophisticated forms of trial and error learning.

The two theories have been contrasted as "pessimistic" -- **NAT**s contention that disaster is inevitable in badly designed systems, versus "optimistic" – **HRO**s pragmatic approach to achieving greater reliability. The theories, however, are in agreement as to which characteristics of systems make them accident prone. This study will examine whether the best practices advocated by HRO theory were implemented at Fukushima before, during, and after the disaster.

## Lally's Target and Shield Model

Lally (1996) argued that Normal Accident Theory was a sound theoretical perspective for understanding the risks of technology, because technology is complex, tightly coupled and often poorly controlled. She also argued (Lally, 1997) that technology based systems do not operate in isolation but in organizational settings where failures in technology can lead to more widespread secondary failures in organizations and to society as a whole. Additionally, she argued (Lally, 2002) that the frequent rapid change in both technology based systems and the work processes they support can further exacerbate the potential for disaster.

Lally (2004) further extended the model and argued that technology based systems are not only a **target,** used as a weapon of destruction to cause serious accidents, but also a **shield** used to prevent damage from future incidents/whether they be caused by human error, technology based, or from natural causes.

This **"Target and Shield"** conceptual model drew on insights from the Theory of High Reliability Organizations and it suggests that technology designers and managers, as well as government and law enforcement agencies learn from past experiences and embody this knowledge in the design and implementation of future technology based systems. The resulting systems should not only be more secure and resilient, but also be able to prevent future technology based/physical attacks, and mitigate their impact should they occur.

The Target and Shield model incorporates Lally's extensions to Normal Accident Theory. The model also contains *three significant feedback loops*, which allow technology to play a positive role in preventing future incidents from materializing, having real world impacts, and limiting their impacts when they do occur. In 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 Feedback Loop #3, **Mitigate Impact of Disasters**, technology based systems can be developed to prevent accidents resulting from technology based or physical attacks from propagating even further, and to provide more rapid recovery and renewal of culture and quality of life.

## Extensions of Crisis Compliance

Lally extended her Crisis Compliance framework to encompass: 1) Whether technology is the Source, Prevention, or Cure of the Crisis, 2) Crises in Socially Diverse Areas, 3) Unprecedented Crises, 4) Crises with Malevolent Causes, and 5) Post Crisis Infrastructure Rebuilding and Cultural Renewal. These extensions allow the Crisis Compliance framework to encompass a wider range of disasters and raise additional issues for the use of technology to predict, prevent and prevail over the crises.

## Is Technology the Source of the Crisis, the Prevention, or the Cure?

Lally (2008) argues that an important characteristic of a crisis is the role of technology—is it the source of the crisis, the prevention of the crisis or the cure? Lally (2014) states that Y2K had its foundation in poor software design and the rapid expansion and proliferation of technology, making technology the source of the crisis. However, technology played a major role in solving the problem as well. Testing methodologies helped isolate potential failures; the resulting improved methodologies, for developing and documenting systems, lead to more robust systems in the future. Hurricane Katrina and the earthquake and tsunami in Fukushima were natural disasters in their original form. However, the events at Fukushima cascaded into a disaster where man made technology played a major role. Technology methodologies that were already available, could have played a much more successful role in combating the crisis than they did.

## Extending the Model to Crises in Diverse Areas

An additional finding 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 being limited to just 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 (2004a) addressed the challenges of extending the models to large diverse environments, other than organizational settings. Large areas add additional layers of complexity and tight coupling when compared to organizational settings. In organizational settings, the shared mental models recommended by High Reliability Theory are easier to enforce. Organizations can appoint professionals who are educated in preventing disasters and involve all employees in disaster training. Murphy (2004) argued that terrorist attacks in urban areas are likely to involve "a spectrum of trained professionals, cognitively and physically fatigued individuals, motivated volunteers, and frightened victims" (Murphy, 2004, p .2), making shared mental models harder to achieve and appropriate social interaction more difficult. A heterogeneous environment, therefore, provides additional challenges in a crisis. Sargut and McGrath's (2011) complexity model also encompasses diversity as another factor that increases complexity.

The complex, tightly coupled infrastructure of large urban areas makes fault isolation and system restoration more difficult to achieve, exemplified by the blackout of 8/14/03 and Hurricane Irene. IT based initiatives for combating terrorism must address these new challenges as well. Ulmer, Sellnow, and Seeger (2011) indicate that achieving good crisis communication and disaster response was much simpler in Oklahoma City after the

bombing, than in New York after 9/11, because the culture was more homogeneous.

The Fukushima disaster caused radiation leaks that spread throughout large portions of Japan due to radioactive exposure extending beyond the geographical boundaries of Japan. Although Japan has a relatively homogenous, law abiding culture, the global ramifications of nuclear disasters across widely diverse populations must be considered when deploying nuclear power technology.

**Unprecedented Crises Pose Greater Challenges**

Another characteristic of crises that adds to the potential for damage is whether or not they are unprecedented. Lally (2014) argues that Y2K had no precedent, making the challenge of understanding the problem, even by experts, more challenging. Maintaining information transparence with the public also became a greater challenge, since the potential consequences of the problem were not readily determinable.

Crises such as 9/11 and Hurricane Katrina were not beyond imagination but were unprecedented on the scale at which they occurred (Lally, 2006), (Lally & Garbushian, 2007). Despite 130 years of technological advances, civil reform, and building code updates, the Fukushima disaster resulted in 20,000 deaths and a major nuclear accident whose impacts are still being calculated (Katayama, 2011).

As a result of a crisis being unprecedented, there was no collection of best practices to draw on. Developing a theoretical model that allows crisis managers to draw on best practices from cases that are without precedent, but share similar characteristics, will help prevail over an unprecedented crisis. A careful post crisis analysis will reveal additional best practices and establish precedents for future crises.

**The Challenge of Malevolent Threats**

Another characteristic of crises is whether they are the result of malevolent actions. Y2K was caused by an inadvertent error by program designers. The result of extensive Y2K testing has led to better software design. Lally (2004) argues that 9/11, in contrast, 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. When a recent Germanwings air disaster was determined to have been deliberately caused by the co-pilot, a different model of the role of technology's use in preventing the disaster emerged. The focus now centered on gathering information about the psychological state and the intentions of the operator of the airplanes, rather than the technology of the airplanes themselves (Kulish, Eddy and Gray, 2015). Fukushima was not malicious, because even the harshest critics of the government's policy don't suggest that anyone wanted it to happen.

However, a nuclear power plant disaster could be caused by malevolent individuals with inside information about the plant's operations and/or with weapons such as bombs or hijacked airplanes. The impact of these attacks could hypothetically be much worse than those experienced at Fukushima and are well within the realm of human imagination.

## Post-Crisis Renewal: Rebuilding Infrastructure and Restoring Culture

Lally (2013) argued that in the wake of natural disasters such as Hurricanes Katrina and Sandy, technology provides several technological and methodological solutions to recover from the disaster and to build a more resilient environment in the future. She argues that stakeholders must make informed decisions about the feasibility of available solutions. Individual stakeholders in the Post-Crisis environment must make informed decisions between rebuilding in the same areas or relocating elsewhere.

Lally (2008) also argued that technology can be the source of Post Crisis recovery and renewal. She cited examples of how survivors of Hurricane Katrina used the Internet to locate friends and relatives and to create support groups among geographically disbursed survivors. Lally and Ahad (2009) applied her model to survivors of the wars in Afghanistan. She conducted a study that indicated that individuals exposed to positive multimedia images of the beauties, rather than the tragedies of Afghan culture were more likely to support non-military aid. The use of technology as a force in Post Crisis Renewal appears to be affected by the strength of the affected culture and by the number of positive images, sounds and other sensations associated with the pre-disaster culture. Japan's long and rich cultural heritage should provide a great source of Post Crisis renewal in the Post Fukushima environment.

## Characterizing Fukushima in terms of Crisis Compliance

Fukushima can be characterized in terms of the Crisis Compliance framework to provide a foundation for understanding its emerging implications that extend the models.

The Fukushima disaster began in March of 2011 when a major earthquake hit Northeastern Japan, causing a major tsunami. (Lochbaum, Lyman, Stranahan, 2014). Sensors throughout Japan indicated that an earthquake was imminent and alerted the Fukushima Daiichi plant. The plant responded to the earthquake with a "by the book scram" shutdown, coping successfully with this more anticipated and planned for event.

However, the tsunami resulting from the earthquake overflowed the restraining wall and flooded the plant, damaging all reactors and disabling both regular and backup power sources. This is an example of the "common mode" failure Perrow warned about. Not only were primary systems disabled, but also all backup systems and safety indicators in the control room—which was left completely in darkness. The quick, courageous and innovative responses of the plant's managers and workers created rigged solutions that prevented the impacts of the disaster from being even worse than it could have been. However, the damage to the plant resulted in a nuclear meltdown and radiation release whose impacts are still being measured. In addition to nearly 20,000 people being killed by the earthquake and tsunami, millions of people had to be relocated, including several entire villages. Increased levels of radiation have been detected as far away as California.

In terms of Normal Accident Theory, the original disasters of the earthquake and tsunami, like Hurricane Katrina, were natural in origin and were predictable in advance. Unlike Hurricane Katrina, the natural disaster, was greatly compounded by the impact of the tsunami on the complex, tightly coupled technology of the Fukushima nuclear power plant, creating a new kind of disaster. As a result, the Fukushima Nuclear Independent Investigation Commission called the events at Fukushima "a profoundly man-made disaster" (Tabachi, 2012, p. 1) that could have been foreseen and prevented. The disaster was

described as a "special event," that had "never been envisioned," that was "beyond the procedure manual," and "beyond what we trained for," by the workers at the Daiichi plant (NOVA, 2015).

In accordance with High Reliability Organization theory, procedures were in place for coping with the earthquake but they may not have been sufficient given its strength. The combination of the earthquake and tsunami was not planned for, although there was significant historical precedent of earthquakes giving rise to tsunamis. The scale of the tsunami was also beyond the scope planned for, and procedures for preventing and responding to blackouts due to mass flooding was not well thought out. Once major damage had occurred and a meltdown had begun, Fukushima also lacked the methodologies for coping with an extreme emergency. The Japanese government also failed in its obligation to alert the public and address the crisis.

In terms of the Target and Shield Model, the Fukushima disaster failures caused by the earthquakes and tsunami propagated into a nuclear meltdown with widespread societal and economic impacts. In terms of using technology to mitigate the disaster, the power failure left most technology based solutions unworkable, "We were facing an unseen enemy," armed only with a "broken safety culture" (NOVA, 2015). Like 9/11, this disaster that was not unimaginable but was considered so unlikely that a detailed response had not been crafted. Its occurrence had changed the rules of disaster response.

With regards to the three feedback loops, all aspects of preventing future disasters: 1) predicting and preventing future incidents, 2) preventing propagation of incidents and 3) mitigating the impact of future disasters, must be addressed. Lally (2008) argued that after 9/11 a number of technological innovations for detecting potential terrorist threats and assisting first responders were developed that have already found additional applications in other crisis scenarios. Lally (2013) also argued that regions that survived Hurricane Sandy had a number of hurricane mitigation technologies to choose from that were already functioning in areas such as the Netherlands.

30 out of 100 nuclear plants currently active in the U.S. are built on the same design as Fukushima. $2 billion have been dedicated to develop new safety technologies and methodologies (Halpern, Channon, and Wald, 2014). The success or the failure (Saito, Takenaka, and Topham, 2013) of these technologies can provide insight into the need for enhanced safety practices required to make nuclear energy viable. However, technological solutions developed and implemented thus far at Fukushima have met with limited success, with Japanese auditors reporting that a third of the $1.6 billion in taxpayer money has been wasted. A "lack of transparency" in the process of choosing contractors to develop containment and cleanup technologies was held partly to be blamed (Associated Press, 2015).

Five years after the disaster, contaminated water continues to flow from the site into the ocean, and "the technology to scoop melted fuel out of the damaged reactors doesn't even exist yet" (Featherstone, 2016, p. 2). Chief decommissioning Officer Naohiro Masuda still reports that "At Fukushima Daiichi, there's no textbook" (Featherstone, 2016, p.1).

There are several parallels that emerge when comparing Fukushima, Y2K, 9/11, and Hurricane Katrina (Brinkley, 2006), (Lally, 2006), (Lally & Garbushian, 2007). For example, similar to Y2K when it was first discovered, the dimensions of the disaster were "unknowable". However, unlike Y2K, which had a clear deadline, the Fukushima disaster resulted in some areas of the nuclear plant being radioactive till date and it still cannot be

examined to discover the exact sequence in which the disaster occurred, or the full extent of the damage.

Like Hurricane Katrina, both crises occurred in affluent, well-educated countries with experts available who were able to (and often did) address these issues before the disasters occurred (Van Heerden, 2006). In both cases, information from top down sources was ignored by decision makers, and information from bottom up sources before the disaster was unavailable to stakeholders. Unlike Hurricane Katrina, which was a natural disaster, Fukushima was a cascading disaster that involved a pair of natural disasters evolving into a technological one.

As in the case of 9/11, the Fukushima disaster required a massive cleanup effort. In both cases, the cleanup effort involved exposing workers to a toxic environment whose negative health impacts were stochastic—not manifesting until later, and not in a uniform way across the population of exposed workers. At Fukushima, a $5 million device, that uses X-ray like technology to locate molten fuel debris without exposing workers to radiation, is not yet operational (Associated Press, 2015a). Determining the degree of information transparency, versus concealed risk the workers faced when deciding to join the cleanup effort, are key issues for any massive cleanup effort in a toxic environment. Unlike 9/11, where cleanup workers were characterized as heroes (DePalma, 2011), Japanese cleanup workers are stigmatized as being contaminated by their exposure to radiation (Chao and Barnett, 2012), (Tabachi, 2014). Radiation contamination will leave whole communities uninhabitable for at least 40 years and require new and innovative methodologies to decommission the plant.

Going forward, what are the obligations of organizations and governments to their stakeholders to address problems that are identifiable and fixable before disasters occur? If the timeline of the crisis is set from the moment the tsunami hit, the responses of the plant workers to an out-of-the-box disaster were admirable and resulted in minimizing the impact of a terrible situation. However, decisions about the future of the nuclear power industry must be made in terms of the game changing events at Fukushima. Are individuals, organizations and governments being given complete information in addressing these important decisions, or, is information being withheld, making optimal decisions less possible? What additional information do stakeholders require before deciding to move near a nuclear power plant? Is nuclear power so inherently unsafe and the impacts of disasters so devastating, that the technology is not viable?

## Extending Dimensions of Crisis Compliance in the Wake of Fukushima

An analysis of the Fukushima disaster raises a number of emerging aspects of Crisis Compliance. They include:

1. "Design Basis" versus "Beyond Design Basis" risks.
2. Deterministic versus Stochastic Risks
3. Physical and Geographic Scope
4. Contained versus Cascading Disasters
5. Internal versus External Locus of Control

## "Beyond Design Basis" Risks

Two additional concepts emerge from a study of Fukushima that are essential for understanding the degree of risk in a scenario characterized by complex technology. The concepts are "Design Basis" and "Beyond Design Basis" and can be applied to any complex technology based system. Design Basis Risks are those that can be, to a reasonable degree, expected to occur with a given technology, and therefore, must be taken into account in their design and manufacturing by vendors. Examples include flat tires on cars and trash fires in large buildings. Designers of these systems are expected to address these anticipated risks with coping technologies and methodologies to prevent their occurrence and minimize their impact.

Beyond Design Basis risks are those "out of the box" risks that lie outside the realm of what can reasonably be expected to occur. Due to their unexpected nature, they have no clear precedents from which best practices can be drawn and no immediate technological or methodological solutions. Disaster response becomes a much more challenging problem. Y2K and 9/11 can be clearly characterized as "beyond design basis" disasters at the time of their occurrence, because they had no clear precedent at the time they occurred. However, because of these disasters, expanded definitions of "design basis" risks emerged and required new technological and procedural methodologies for responding to these classes of crises. New disasters make future disasters more foreseeable. Manufacturers of complex technologies can no longer cling to overly optimistic definitions of Design Basis Risks when confronted with the actual consequences of risks that have already materialized.

Issues that emerge include: 1) Whether the definition of "design basis accidents" applied in the Japanese nuclear power industry was realistic, given the knowledge available at the time of the Fukushima disaster, 2) How the events resulting from the tsunami at Fukushima have expanded the concept of "design basis accidents" in the nuclear power industry, and 3) How Crisis Compliant power plants must respond in the future. Other recent examples of overly optimistic definitions of "design basis accidents," include the December 2013 Amtrak train wreck in upstate New York, and the 2016 crash of a commuter train in Hoboken, where a fatal accident occurred, despite the availability of technology to remotely stop the train (McGeehan, Rosenberg, and Fitzsimmons, 2016).

## Deterministic versus Stochastic Risks

Another major distinction in risk analysis hinges on whether the negative outcome is virtually guaranteed to happen once the disaster has occurred and whether it is visible and measurable when it happens. If so, the risk is called "deterministic." With deterministic risk, the outcomes are observable and the negative outcome follows a clear path of causality within in an observable time frame. An example of deterministic risks would be a homeowner having an icy sidewalk and a passerby falling and breaking his ankle.

The second class of risk is called "stochastic risk." In stochastic risk, the negative results do not automatically follow in a clear causal sequence. They may take years to emerge, or may not manifest at all. In this case, the icy sidewalk is still there but no one has fallen on it yet. Other examples include the impact of smoking on cancer, and the impact of exposure to dust (during the cleanup of Ground Zero after 9/11) on emphysema among cleanup workers. Attributing causality and the resulting liability in these scenarios is much

more problematic. Much time and energy can be spent on investigations to prove who is responsible, who has been victimized, and how much the injured parties can recover.

In the case of nuclear power, when radiation exposure exceeds a threshold value, usually in the tens to hundreds of rems, the results are deterministic. The radiation kills cells and damages organs causing "acute radiation syndrome," resulting in death. The impacts of severe exposure to radiation over a short period of time are, therefore, deterministic.

When the radiation exposure is below the threshold value, the risks of the exposure are definitively stochastic. The radiation does not definitively cause the exposed individual to immediately experience illness or death. Therefore, the link between exposure and illness is not as clear in terms of causality. Other factors can come into play such as the individual's lifestyle or pre-existing conditions that may impact the individual's response to the exposure and resulting longevity. Exposure to radiation, or to the dust at ground zero after 9/11, or the prolonged effects of alcohol and tobacco are other examples of factors that gave rise to impacts that have been debated because of their non-deterministic nature.

At Three Mile Island and Chernobyl, debate continues over the long term impact of the radiation released by the accidents, and its impact on public health and the future of nuclear power. Japan is currently struggling with the issue of studying the impacts of Fukushima's fallout on exposed populations (McNeill, 2014). A key emerging issue is the obligation of governments to disseminate information regarding deterministic and stochastic impacts of nuclear risk factors to allow individuals to make informed choices about the radiation risk they now face, and to choose among alternative energy sources in the future

**Crises and Physical Geographic Scope**

Another characteristic of crises is their physical geographic scope. 9/11 was a major disaster in terms of loss of life and property, and was due to malevolent causes. However, the physical damage was limited to several square miles. Physical and Geographic scope addresses whether the crises can be controlled by quarantining the area, and whether the effects of the crisis spread quickly beyond its original geographic boundaries. Sites like Chernobyl were remote and were able to be quarantined, resulting in limited impact outside the affected area. Quarantining and evacuating a densely populated area such as Japan presented far greater challenges. 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. Four years later, trace amounts of radiation from the disaster are still being reported in Canada (Reuters, 2015).

**Contained versus Cascading Disasters**

Disasters can not only happen in one isolated time and place, but also may lead to *other disasters of a different nature* that occur *at separate locations, at separate times*, and give rise to their own consequences. These *disaster trails* can be explained in terms of the Target and Shield Model, where isolated failures, unless contained, give rise to system wide and even global risks. In Japan, the earthquake and tsunami were disasters in their own right. The death toll for these disasters was over 15,000 with massive destruction of property and displacement of entire communities. It was against this backdrop that the nuclear meltdown

took place. Although cascading disasters need to be analyzed individually, their interactive and compound effects result in even more devastating consequences.

In recent financial history, the failure of the U.S. sub-prime housing market contributed to a number of other business and financial failures with wide ranging negative social consequences. If disasters are not contained, they often give rise to financial crises, epidemics, and population relocations that have enduring repercussions. Understanding the relationships between cascading disasters is important in containing their impact. Creating buffers to protect essential assets from the indirect impact of disasters beyond a given individual's, organization's or government's sphere of control is another key aspect of crisis compliance. The question arises as to how wide the span of control a Crisis Compliant organization can have to protect itself against cascading disasters.

## Internal versus External Locus of Control

Crisis Compliance argues that organizations and governments must take responsibility for their own crises, based upon an active examination of the risks in the environment. Compliant organizations cannot rely on external agencies, customer complaints, or actual disasters to make them aware of problems. When organizations become too closely allied with their regulatory agencies, a moral hazard is created, permitting governing agencies and affected organizations to collaborate in creating more limiting regulations. In Japan, the relationship between TEPCO and the NRC permitted limited definitions of "beyond design basis" accidents, which limited the preparedness needed at Fukushima. Organizations that: take an adversarial attitude toward complaints, hoping for the best, and respond with improved technologies and methodologies, only when legally necessary, are not Crisis Compliant. Compliant organizations cannot pursue a passive policy of responding only to external forces; they must enforce an active anti-disaster policy of their own.

## Conclusion: Crisis Compliance Post Fukushima

This paper has presented a theoretically based framework for characterizing IT based threats and opportunities. A twelve-part framework of key characteristics of crises emerged. Characteristics with an asterisk have emerged from the present analysis.

1. Is the crisis on an individual, organizational, or global level?
2. Are technology based systems the target of the threat and/or can technology be used to combat the threat?
3. Is the crisis occurring across a heterogeneous population or one with a common culture and language?
4. Is the crisis unprecedented? What can we learn from best practices in dealing with previous crises?
5. Is the crisis being caused deliberately by malevolent people or a result of an inadvertent error or natural disaster?
6. What technology based solutions are currently feasible, and to what degree are individuals, organizations and government leaders obliged to use them? What are the ethical and legal implications of not using them?
7. *Is the crisis "beyond design basis" for the technology involved?

8. *What are the deterministic versus the stochastic risks of negative outcomes?
9. *Can we contain the physical geographic scope of the crisis? How far and how fast can it spread?
10. *Is the crisis of a single type (natural disaster or technological failure) or are cascading disasters involved?
11. *Is the current crisis environment characterized by internal or external control?
12. What are the long term impacts of the crisis and how can technology help restore the quality of life and culture once the crisis has passed?

In terms of the original Crisis Compliance framework, Fukushima was a textbook Normal Accident scenario—a complex, tightly coupled system, which experienced fatal common mode failures that resulted in a loss of control. In terms of HRO, the failure of imagination in envisioning the source and severity of the crisis made existing crisis response methodologies inadequate. Likewise, the technology based methodologies for mitigating the impact of the disaster were crippled by the common mode failures that caused the blackout.

All the emerging crisis characteristics make nuclear power more disaster prone. Fukushima, quickly propagated into a "beyond design basis" crisis making existing procedures inadequate. The radiation leaks resulting from the disaster had serious stochastic implications for the health of individuals exposed. Radiation leaks were difficult to contain geographically. The Fukushima event was a cascading disaster, where one disaster evolved into another, each exacerbating the impacts of the others. There are major concerns about who should regulate the nuclear power industry. These critical factors all point to a reconsideration of the decision to use nuclear power. Future research will address the key issue that emerges from analysis: Crisis Compliance needs to encompass making an informed and transparent decision about the potential risks involved in creating or entering a disaster prone scenario in the first place.

## REFERENCES

Associated Press (2012), Italy Disaster Expert Quit Over Quake Trial. October 23.

Associated Press (2015). Japan Audit: Millions of Dollars Wasted in Fukushima Cleanup. *New York Times*. March 24.

Associated Press (2015a). Technology to Look Inside Fukushima Reactors Faces Challenge. *New York Times*. March 27.

Banks, J., & Coutu, D. (2008). How to Protect Your Job in a Recession. *Harvard Business Review, September*, 113-119.

Brinkley, D. (2006). The Great Deluge: Hurricane Katrina, New Orleans, and the Mississippi Gulf Coast. New York: Harper Collins.

Chao, T. & Barnett, S. (2012). Shunned Japanese Fukushima Plant Workers Face Emotional Toll. *ABC News, August 15.*

DePalma, A. (2011). *City of Dust: Illness, Arrogance, and 9/11*. New Jersey: FT Press.

Featherstone, S. (2016). Fukushima: Five Years Later. *Popular Science*. March-April.

Grabowski, M. & Roberts, K. (1997). Risk mitigation in large scale systems: Lessons from high reliability organizations. *California Management Review, Summer,* 152-162.

Halpern, C., Channon, H., & Wald, M. (2014). Lessons from Fukushima. *New York Times Video, March 9.*

Katayama, L. (2011). Quake Ready Japan. *WIRED. May*. 44-45.

Klein, R.L., Bigley, G.A., & Roberts, K.H. (1995). Organizational Culture in High Reliability Organizations. *Human Relations*, 48:7. 771-792.

Kulish, Nicholas., Eddy, Melissa, Gray, Nicola. (2015). Germanwings Pilot Searched Web About Suicide and Cockpit Doors. *New York Times*. April 2.

Lally. L. (1996). Enumerating the Risks of Reengineered Processes. *Proceedings of 1996 ACM Computer Science Conference,* 18-23.

Lally, L. (1997). Are Reengineered Organizations Disaster Prone? *Proceedings of the National Decision Sciences Conference,* 178-182.

Lally, L. (1999). The Y2K Problem: Normal Accident Theory and High Reliability Organization Theory Perspectives *Proceedings of the 1999 National Decision Sciences Conference*, 234-237.

Lally, L. (2002). Complexity, Coupling, Control and Change: An IT Based Extension to Normal Accident Theory. *Proceedings of the International Information Resources Management Conference.*

Lally, L. (2004). Information Technology as a Target and Shield in the Post 9/11 Environment. *Information Resources Management Journal, 14(1)*, 12-24.

Lally (2004a), Information Technology as a Target and Shield in Urban Environments, *Proceedings of the AMCIS Conference.*

Lally, L. (2006). IT Based Opportunities and Threat: The Appropriate Role of Government. *.International Journal of Technology, Knowledge, and Society. 2(3).* 17-24.

Lally, L., & Garbushian, B. (2007). Crisis Compliance: Hard Lessons from Hurricane Katrina. *Proceedings of the National Decision Sciences Conference.*

Lally, L. (2008). Crisis Compliance: Using Information technology to Predict, Prevent, and Prevail Over Disasters. *Journal of Information Technology Research. 1(1).* 34-46.

Lally, L. (2008a). Information Technology and Post-Crisis Renewal. *International Journal of Technology, Knowledge and Society, 4(1).* 7-14.

Lally, L. & Ahad, M.. (2009). Delight and Disaster Relief through the Use of Multimedia. *Journal of International Business and Law, 8(1)* 91-98.

Lally, L. (2013). Information Technology and Crisis Compliance: Implications for Studying Hurricane Sandy. *Proceedings of the Northeast Decision Sciences Conference.*

Lally (2014). Information Technology and the Clinton Administartion: Proactive Leadership in Turbulent Times. *A True Third Way? Domestic Policy and the Presidency of William Jefferson Clinton.* 1-7.

LaPorte, T. R. & Consolini. P. (1991). Working in Practice But Not in Theory: Theoretical

Challenges of High Reliability Organizations. *Journal of Public Administration, 1,* 19-47.

Lash, J. & Wellington, F. (2007). Competitive Advantage on a Warming Planet, *Harvard Business Review, March,* 95-100.

Lochbaum, D. Lyman, E., & Stranahan, S. (2014) Fukushima: The Story of a Nuclear Disaster. New York: The New Press.

McGeehan, P., Rosenberg, E., and Fitzsimmons, E., (2016). Hoboken Train Crash Kills 1 and Injures Over 100. *New York Times* (Sept 29).

McNeill, D. (2014). Concerns over Measurement of Fukushima Fallout. *The New York Times, May 21.*

Mitroff, I. (2005). Why Some Companies Emerge Stronger and Better From a Crisis. New York: AMACOM.

Murphy, R. (2004). Rescue Robotics for Homeland Security. *Communications of the ACM,* March, 66-68.

NOVA. (2015). Nuclear Meltdown Disaster. PBS.

Perrow, C. (1984) *Normal Accidents: Living with High Risk Technologies,* New York: Basic Books.

Roberts, K. (1989). New Challenges for Organizational Research: High Reliability Organizations. *Industrial Crisis Quarterly. 3,* 111-25.

Reuters. (2015). Radiation from the Fukushima Disaster Newly Detected Off Canada's Coast. *New York Times.* April 7.

Sagan, S. (1993). The Limits of Safety. Princeton New Jersey: Princeton University Press.

Saito, M., Takenaka, K., & Topham, T., (2013). J. Japan's "Long War" to Shut Down Fukushima. *Reuters,* March 8.

Sargut, G.& McGrath, R. G. (2011). Learning to Live with Complexity. *Harvard Business Review. September.* 69-76.

Ulmer, R.R., Sellnow, T.L., & Seeger, M.W. (2011). *Effective Crisis Communication: Moving from Crisis to Opportunity,* 2nd Edition. Los Angeles: Sage Press.

Tabachi, H. (2012). Inquiry Declares Fukushima Crisis a Man-Made Disaster. *New York Times, July 5.*

Tabachi, H. (2014). Unskilled and Destitute Are Hiring Targets for Fukushima Cleanup. *New York Times, March 16.*

Van Heerden. (2006). *The Storm: What went wrong and why during Hurricane Katrina—The inside story from one Louisiana Scientist.* Viking Press: New York.

*This research was supported by a Summer Grant from the Frank G. Zarb School of Business at Hofstra Univeristy.*