Asia Pacific Journal of Information Systems
Vol. 29 No. 1 (March 2019), 144-164

ISSN 2288-5404 (Print) / ISSN 2288-6818 (Online)
https://doi.org/10.14329/apjis.2019.29.1.144

IT Manager Behavior in Crisis Response: Understanding Crisis Cases Using Recommendations from the Crisis Management Literature

Tommi Tapanainen[a,*], Olivier Lisein[b], Ryuichi Hosoya[c], Taro Kamioka[d]

[a] *Assistant Professor, Department of Global Studies, Pusan National University, Korea*
[b] *Assistant Professor, HEC Liège, University of Liège, Belgium*
[c] *Ph.D. candidate, Graduate School of Commerce and Management, Hitotsubashi University, Japan*
[d] *Professor, Graduate School of Business Administration, Hitotsubashi University, Japan*

ABSTRACT

In their role as stewards of organizational information technology (IT), IT managers participate in crisis management activities. While much has been said about the power of technology in improving preparation for emergencies, the behavior of IT managers in crisis situations is not well understood. This paper addresses IT manager actions during the crisis response effort, when appropriate actions need to be taken at short notice. Recognizing that few guidelines exist for IT managers in these situations, we use recommendations from the crisis management literature in analyzing five earthquake cases from Japan and Taiwan. We identify several recommendations from this set for IT managers, which are related mainly to communications and leadership behaviors, suggesting that the IT manager role is a vital one in crisis response. The research additionally shows that recommendations from the crisis management literature have value also when applied to IT managers. Finally, we conclude on several ways that our understanding of IT manager crisis response could be developed by future research.

Keywords: Crisis Management, Crisis Response, IT Managers, Leadership, Earthquake

Ⅰ. Introduction

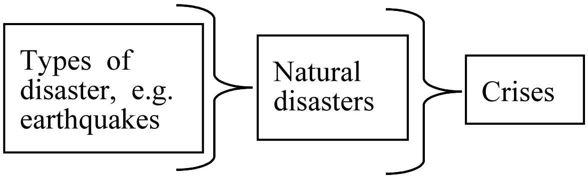
Information technology (IT) has become a basic service for organizations the same way as water and electricity supply (Herbane et al., 2004), and it is the expectation that IT services be available at all times. While this dependency on IT has brought great convenience, it has also introduced a weakness, which becomes evident when IT breaks down as a result of disaster events. Natural disasters can damage data cables and computers, disrupting heavily IT-dependent business services, and making it harder

*Corresponding Author. E-mail: tojuta@gmail.com Tel: 82515103007 for the organization to maintain the continuity of services which are less dependent on IT. It should be underlined that the proper functioning of IT is particularly critical in crisis and emergency situations, because relief efforts during such situations are dependent on the availability of reliable information that is provided when and where it is needed (Comfort and Haase, 2006). For example, a fire occurred in Korea Telecom premises in November 2018, destroying its network equipment and disabling telecommunications services for hundreds of thousands of people in several districts of Seoul, Korea (The Korea Herald, 2018a; 2018b; Hankyoreh, 2018). While no lives were lost, a deeply troubling aspect of this disaster was that not only business services, but also critical services such as emergency telephone services and hospital computing services suffered temporary outages. It is not difficult to imagine that such impacts can lead to very serious consequences very quickly. Hence, the management and rapid recovery of IT services in crisis situations is paramount; not only to recover business services reliant on it but to coordinate the recovery effort itself. The ability to manage information has been found to be invaluable e.g. in coordinating supply chains during large-scale natural disasters (Day et al., 2009).

Crisis is defined as an unexpected and damaging event that is comparatively rare (Boin et al., 2005; Ulmer et al., 2007). Natural disasters can be the cause for crises, but crises can also result from intentional or unintentional human activity, for example industrial accidents and terrorist attacks (Lewis, 2006). <Figure 1> illustrates the relationship of the concepts of crisis, natural disaster, and specific disaster type, such as earthquake.

Crisis management is the effective resolution of a crisis situation by taking three distinct steps: preparation before the crisis, response during the crisis, and recovery after the crisis (Lettieri et al., 2009). Much interest in the IT literature related to crisis management either focuses on preparations to develop IT artifacts for crisis management or analyzes crisis cases that lead to recommendations for the design of IT artifacts. Although such efforts are valuable, due to the unexpected nature of crises, mechanically following pre-planned instructions is insufficient (Drabek and McEntire, 2003; Turoff, 2002). Therefore, any artifact will include a number of assumptions that may not correspond to actual future situations. Appropriate leadership during crisis response can leverage human ingenuity and adaptability, and can therefore overcome unexpected situations where preparations have not been sufficient. Leader actions also address the emotional side of crises, as followers look to their superiors for support in the confusion and bafflement (Devitt and Borodzicz, 2008; Weick, 1990).

Large-scale flooding occurred in Thailand in 2011. Thousands of factories were damaged and forced to halt production activities, including Japanese IT firms such as Sony, Canon, and Hitachi (Aon Benfield 2012; Kawamura 2012). While infrastructural prepa-



<Figure 1> The concepts Disaster Type, Natural Disaster, and Crisis

rations were inadequate, human actions during the crisis did help alleviate the consequences. In some multistoried factories, staff reacted quickly and transported sensitive and expensive equipment to higher floors (in cases where such equipment were not too large to be moved) to reduce the damage caused. In other factories, oil coating and plastic sheets could be applied to some machinery to lessen water exposure. Such actions often saved the equipment from having to be replaced in a demand-glut situation right after the crisis. However, as it took around two months for floodwaters to recede and factories to start operating once again, affected companies still suffered great losses.

Crisis management has been extensively studied in connection with large-scale societal crises, but to a lesser extent as an activity in the IT units of organizations. Despite the abundance of attention to technologies as a resource to overcome disastrous events (Lettieri et al., 2009), the behavior of the IT manager during crisis response remains poorly understood. Because IT managers hold the key to successful resolution of crisis events within IT units, it is critical that IT managers have the necessary awareness, training, and ability to act in crisis response. The lack of adequate preparations lies at the foundation of the two example disaster stories told in this section. Despite this, the Thai flooding story also shows how smart and resolute actions in the face of unforeseen situations – which have not necessarily been rehearsed as part of business continuity plans or incident response guidelines – can make a difference.

Therefore, this research focuses on exploring the research problem "how IT managers behave in crisis response" through a number of actual crisis cases that have occurred in organizations and their IT units. It does so by 1) collecting qualitative data through interviews addressed to IT managers, and 2) using the existing recommendations given for organizations in crisis response as a tool in analyzing this data. Through such analysis, it identifies IT manager crisis response behaviors that relate to the recommendations given in past literature, showing which behaviors were relevant particularly for IT managers in the given set of interviews. This understanding guides research on IT manager leadership by showing which behaviors should be prioritized and require particular attention in crisis situations, a situational type that exhibits a dearth of empirically founded theorization in IT manager leadership. It also informs research in crisis response information exchange, where IT managers hold critical roles. The five cases in this paper are all derived from earthquakes in Japan and Taiwan, as explained in the research method section.

The paper is structured as follows: in section two, the existing literature is reviewed on IT manager behavior and its link to crisis situations, as well as prior recommendations given for crisis response. Section three explains the research method and design. Then, in section four, the case contexts are explained, and in section five, the recommendations for crisis response found for each case are presented. The two remaining sections focus on discussion (section six), and contributions, limitations, and future research (section seven).

Ⅱ. Literature Review

2.1. What Do We Know and Not Know About IT Manager Behavior in Crisis Situations?

There have been some attempts at comprehending the role of IT functions in crisis situations (<Table 1>). Often, these investigations have focused on the use of technology to predict or mitigate a crisis. For example, Housel et al. (1986), Jennex (2004), McKinney (2008), and Thomas et al. (2009) describe the characteristics of information systems for crisis management. Such articles focus on technological artifacts. Another strand of research has focused on a wider perspective, the types and characteristics of information networks that are used in communications between stakeholders during crisis response (Comfort et al., 2010; Harnesk, 2013; Pan et al., 2012; Xue and Liang, 2004). A third approach is yet wider; it investigates the organizational arrangements in crisis management where IT is an enabling property. Examples of this kind of articles are the work of Calloway and Keen (1996), who illustrate the role of corporate IT as an organizing resource during crises using the cases of Exxon Valdez and the Gulf War, and the reports of Devadoss and Pan (2004) and Leidner et al. (2009), who provide an interesting look at how the Singapore government agencies managed the SARS and Asian Tsunami disasters.

Although the above shows that a number of articles have addressed how crisis situations unfold in relation to IT functions, the literature has shown markedly less interest on IT manager behavior in crisis situations. It is possible, however, to try to use extant literature to obtain indirect information regarding this. One such approach is through the content of business continuity plans and other similar plans made by organizations. Andrews (1990) is among the few scholars reporting on this. He states that an effective disaster recovery plan should contain a step-by-step list of processes and actions to be taken during the emergency, including measures for the continuity of telecommunications and the recovery of backup files. This is in line with Hecht (2002) who states that the two primary requirements of business continuity are the availability of data and connectivity of the network. The plan would also include the contact information of key personnel and vendors. The above implies that the IT manager would at least be required to recover the data and make it available for the stakeholders, which probably requires a degree of urgent communication and col-

<Table 1> Overview of Related Research on IT Manager Role in Crisis Management in the Field of Information Systems

Example papers	Topics addressed
Housel et al. (1986), Jennex (2004), McKinney (2008), Thomas et al. (2009), Ashir (2014), Pee and Lee (2016)	Characteristics of information systems for crisis management; giving recommendations for the design of such systems
Xue and Liang (2004), Comfort and Haase (2006), Comfort et al. (2011), Pan et al. (2012), Harnesk (2013)	Types and characteristics of information networks that are used in communications between stakeholders during crisis response; analyzing and hypothesizing outcomes of crisis collaboration using such information networks
Calloway and Keen (1996), Devadoss and Pan (2004), Leidner et al. (2009)	Organizational arrangements in crisis management where IT is an enabling property; giving accounts of crisis cases and proposing lessons learned
Andrews (1990), Hecht (2002)	Planning and preparations for business continuity in case of disruptions and disasters affecting IT; crisis response less addressed
Applegate and Elam (1992), Chen et al. (2010)	Skills, characteristics, and behaviors required of IT managers and CIOs mostly in stable situations; crisis situations less addressed
Wang and Belardo (2009), Day et al. (2009)	Information processing and flow in crisis situations

laboration with internal and external parties. The type of actions taken in the procedure, and the nature of communication and collaboration is, however, not yet clear.

The concept of Chief Information Officer (CIO) leadership, examined by Applegate and Elam (1992) and Chen et al. (2010), can also provide some insight as to how IT manager behavior should be conceptualized in crises. Applegate and Elam (1992) argue that investigations of CIO leadership should focus on substantive knowledge and career experiences such as business/organizational knowledge, relationships both within and outside the company, and the IT manager's record in a broad set of activities. To complement the above, they add that more subjective dimensions, such as interpersonal skills, integrity and personal values, and the level of motivation should also be considered. They derive these facets from Kotter (1988)'s writings. On the other hand, Chen et al. (2010) build their definition of CIO leadership on the transformational leadership theory (Bass, 1985). They argue that the categories of human capital, structural power, and organizational support for IT are the three building blocks for IT manager leadership. As may be seen, both definitions consider the IT manager's relationships with other people to be important in IT manager leadership. However, these articles addressed IT manager leadership in stable situations, not in crisis situations.

The role of IT managers as leaders during crisis situations would require attention, because IT managers are in a position to enhance the flow of critical information in the organization during crisis situations. For example, Comfort et al. (2004) found that the availability of core information during crisis situations – which is dependent on the information strategy used – improves the outcome of crisis response actions. Similarly, Wang and Belardo (2009) found that the use of appropriate knowledge strategies during crisis situations contributes to the achievement of crisis management objectives. It is through the provision of relevant information and knowledge by which the value of the IT managers' job is evaluated. IT managers must also resolve problems in organizational information exchange. The report of Day et al. (2009) regarding disaster relief during Hurricane Katrina shows that impediments in information flow can be detrimental to the coordination of resources during crisis situations. The suggested solutions for these impediments include, for instance, prioritization of important information, integration of different information, and searching for new information, activities that often require managerial involvement.

As shown in the report of crises in two Taiwanese energy companies by Wang and Belardo (ibid.), the examination of organizational archives as well as extensive communication among employees was necessary in responding to the crisis situation. Day et al. (ibid.) also report that the manipulation of information stated above does not occur only within IT – it also occurs in the communication among human beings. They state that sometimes the leveraging of personal relationships can be helpful when negotiating difficult procedures between two organizations. These observations emphasize the view that the province of IT managers is also in improving the communications and collaborations links between organizational actors. They are influential in a variety of information and knowledge management activities, and their expertise and experiences contribute to the use of such activities.

While IT managers participate heavily in the above activities, they are also managers in the traditional sense (Ives and Olson, 1981). Therefore, they share many tasks with managers in other departments of the organization, including responsibility for their subordinates, involvement in decisions regarding organizational resources, and communication with external stakeholders such as customers and outsourcing partners. For these reasons, IT managers must be at least as involved in crisis response as do other manager-level members.

2.2. Recommendations Given in Crisis Response

The literature on crisis management outlines a large number of recommendations which organizations should heed. While many recommendations are addressed to the preparation stage (Lewis, 2006), situational variation in crises requires that attention be also focused on the response stage; mere preparations are not enough. According to Lettieri et al. (2009), crisis response consists of actions to manage and control the effects of a crisis and minimize damage. Recommendations on crisis response are focused on a variety of tasks, including awareness of what is going on in the environment, organizing the crisis team and required materials, communicating and collaborating with the team and external stakeholders, and dealing with the psychological effects of the crisis situation (Boin et al., 2005; Lewis, 2006).

Many recommendations are drafted without reference to the specific type of decision-maker that is supposed to follow the recommendations (Lewis, 2006; Perrow, 2007; Ulmer et al., 2007). Others are offered specifically to policy-makers and public sector leaders (Boin et al., 2005, Drennan et al., 2015). The recommendations are claimed to be applicable for a wide variety of crises, including natural disasters, industrial accidents, and deliberate, violent acts such as terrorism (Ulmer et al., 2007). Therefore, the recommendations remain at a level that is general enough to accommodate all these varieties of crisis, while at the same time remaining relevant for a variety of organizational leadership roles, from low-level crisis leaders to top-level CEOs and presidents. The consequence of this is that the application of recommendations is case-specific; the actor should evaluate which recommendations are appropriate for him/her, the organization, and the given crisis case.

We read several books and articles containing detailed recommendations on crisis management, and hand-picked recommendations focusing on managerial actions in the response phase. In doing so, we used the definition of crisis response given above. These recommendations from the literature on what managers should do in crisis response are listed in <Table 2>, below. They are grouped using categories that were suggested by the literature (Boin et al., 2005; Lewis, 2006) and comprise several facets of managerial activities during crisis response. They include the detection of crucial issues (detecting problems), resourcing the response effort (resourcing), making important decisions (decision-making), giving directions to stakeholders (coordinating), giving information to stakeholders (communication), and emotion control during the crisis response (emotion management). They are explained below.

- Crisis response necessitates that weak signals preceding the development of events are sensed so that appropriate measures can be taken. Detecting problems is the capacity to capture these signals. It requires that the leader is able and willing to access not only positive news but also negative news about the state of affairs in the organization.
- Adequate resources must be allocated to the crisis response effort. Prepared resources may not always be sufficient and there should be

an awareness that additional capacity can be mobilized. On the other hand, organizational politics are not absent even in crisis situations, and the leader is better off remembering this, while preparing a log of crisis response actions taken to back him/herself up for the inevitable questions that surface after the crisis has passed.

- Crisis decisions must often be made under time pressure. Nevertheless, decisions should be as high quality as possible, and therefore, the leader should remain calm and show the will to carry out the decisions. Yet, decisions should be informed by the opinions of surrounding organizational colleagues and as much as possible, the perceived opinions of the wider public.
- Coordinating the actors in crisis response involves leadership that is appropriate to the circumstances coupled with active sharing of information to all parties, because information is often at a premium in crisis situations. The leader must also see that coordination remains smooth among the members.
- In communicating with stakeholders, there are certain rules that leaders should follow. The leader must gain the trust of their audiences and focus on the core information in the message, which is stated in terms of what is definitely known at the moment. However, even in the absence of sufficient information, communication should take place as early as possible to reassure the audiences. Uncertainties are to be identified as such.
- The human dimension of crises is evident in the strong emotions that are experienced by the victims. If the leader is present in the field together with the followers, this can help to reduce the feelings of stress and panic. The leader should also show care for the victims by expressing sympathy for their suffering and order treatment for those who are most affected. At the same time, he/she should not forget the toll that exceptional circumstances place on him/herself.

<Table 2> Recommendations Given for Crisis Management During the Crisis Response Phase

Category	Recommendations
Detecting problems	Identification of critical information; capturing even bad news (Boin et al., 2005; Weick, 1988)
Resourcing	Clarifying roles and resources (Janis, 1982); readiness to play political games even in a crisis; documentation of crisis response (Boin et al., 2005); addition of capacity in escalating situations (Cohen, 2003)
Decision-making	Keeping calm; sensing the public view of the reasonable course of action (Boin et al., 2005); multiple advocacy decision-making (George and Stern, 2002); resolute decision-making (Quarantelli, 1997)
Coordinating	Monitor and troubleshoot coordination (Boin et al., 2005); initially task-oriented leadership and later relation-oriented leadership (Lewis, 2006); sharing information with all stakeholders (Quarantelli, 1997); transformational leadership and virtuous leadership (Ulmer et al., 2007)
Communication	Retaining audience attention and confidence (Boin et al., 2005; Ulmer et al., 2007); clear communication focusing on essentials (Coombs, 2007); show consistency and will to resolve crisis; avoid speculation and "no comment" (Drennan et al., 2015; Ulmer et al., 2007); communicate early; acknowledge uncertainty; assure stakeholders that contact will be maintained (Ulmer et al., 2007)
Emotion management	Leader field presence (Benson, 1988); self-control of stress (Boin et al., 2005); express sympathy and condolences (Boin et al., 2005; Drennan et al., 2015; Lewis, 2006; Ulmer et al., 2007); making an immediate crisis intervention (Lewis, 2006)

This particular categorization was devised because recommendations are often activity-based, and are introduced using similar categories in the literature, for instance in the form of "five critical tasks" (Boin et al., 2005), "five crucial functions" (Drennan et al., 2015), crisis communication (Ulmer et al., 2007), and psychological interventions (Lewis, 2006).

The above recommendations may offer a guide to IT managers on how they should act in crisis response situations. It has been found that IT managers have many similarities as managers in other functions (Ives and Olson, 1981), and therefore would be expected to be able to apply these recommendations as other managers would. However, as a clear organizational role has not been specified for the recommendations, it is unclear whether, and to what extent, they are applicable to IT managers. In this research, we aim at investigating IT manager crisis response behavior through the lens of recommendations, and in so doing, extracting relevant behaviors for IT managers.

Ⅲ. Research Method and Design

The above sections point to a gap in the literature on understanding IT manager behavior in crisis response. This research attempts to address the gap by exploring real-life cases of IT manager behavior in crisis response, using recommendations given for general management in crisis response situations as an analysis tool. Our objective is to obtain a list of behaviors that are applicable for IT managers in particular.

As crisis situations are inherently complex (Boin et al., 2005), a great deal of background information is required to understand them. The case research method (Dubé and Paré, 2003; Yin, 2009) is particularly appropriate to understand a complex situation in its context. Five crisis management cases in IT functions were selected for data collection in this research. The "case" in this research is defined as the behavior of an individual IT manager in a given crisis response effort.

Earthquakes are one category of an unintentional crisis; while they are largely unavoidable, the actions of organizations regarding preparations and situational response can make a considerable difference on the damage caused (Perrow, 2007; Ulmer et al., 2007). Many earthquakes often occur repeatedly in the same regions (Perrow, 2007) and a large proportion of crisis management literature addresses natural disasters such as earthquakes, hence, it is useful to examine IT manager behavior during earthquakes to understand their behaviors during crisis situations. The cases in this research were selected because each of them are examples of earthquakes that affect IT functions. In particular, these cases are from Japan and Taiwan, where earthquakes occur more often than in many other areas, and therefore, companies in these areas are thought to have extensive expertise in coping with crises related to earthquakes.

The cases also represent a diversity of industries, illustrating a variety of contexts in which IT managers are acting in their roles. Although the data are from two different cultures, the Globe study of leadership classifies Japan and Taiwan in the same cultural group in terms of leadership style (House et al., 2004), facilitating comparisons among leaders from these two areas. The differences in industry are diminished by the fact that only IT functions are examined – which represent a unified professional domain. For instance, Wu et al. (2004) found that IT managers' activities do not vary significantly for different industries.

Data was collected by interviews with persons who were affected by the crisis and were acting to respond to and contain it. Interviews were semi-structured and considerable latitude was given to the interviewees to bring up their own experiences, emphases, and opinions even if they did not correspond to the researchers' prepared question topics. Data was collected not only from the IT managers themselves, but when possible, also from their immediate subordinates, as this can provide additional evidence (Dubé and Paré, 2003) and verification for the IT managers' comments. Interviewed leaders were all IT managers responsible for crisis response efforts, and interviewed followers were these IT managers' direct reports at the time of the crisis. This approach is hoped to circumvent problems in which data is only obtained from a single source (Dubé and Paré, 2003). The interviews were recorded on tape and ranged from a length of 20 minutes to 1 hour and 20 minutes. Afterward, the tapes were transcribed as text. The cases are outlined below, in <Table 3>.

Interviews focused on a single crisis event in the IT function where the person interviewed was working, and included questions related to describing the crisis event, the interviewee's roles and responsibilities at the time, the relationships among and communication that occurred between the IT manager and subordinates.

A comprehensive analysis was completed on the transcripts using the recommendations identified in the previous section for crisis management in the response phase. The analysis proceeded by assigning labels (Strauss and Corbin, 1990) to sections and passages of these transcripts using the categories of 1) detecting problems, 2) resourcing, 3) decision-making, 4) coordination, 5) communication, and 6) emotion management. When a section or passage in the transcripts corresponded to one of these label categories, a label corresponding to that category was assigned to the section or passage. This process is similar to "pattern matching" (Yin, 2009) and the "open coding" technique in grounded theory research method (Strauss and Corbin, 1990), except that the codes do not emerge from data; they are selected from the label categories above.

Then, the events in the transcripts for each company were checked against the specific recommendations given in each label category, focusing on the IT manager as the agent of action. This showed the relevance of label categories to each company case, but also to an extent revealed whether given recommendations were followed or not followed by IT managers in each company. The results of this analysis process are reported below in section five. The process of assigning labels and determining the match against recommendations was conducted by two researchers independently, and the decision on each item was established only after viewing both researchers' analyses.

<Table 3> Summary of the Cases

Company	Country	Industry	Persons interviewed	Leaders/followers
AUTO	Japan	Auto-mobile	2	1 manager and 1 follower
INSURE	Japan	Insurance	3	1 manager and 2 followers
SERVICE	Japan	Business services	2	1 manager and 1 follower
BANK	Taiwan	Finance	1	1 manager
TELCO	Taiwan	Telecoms	3	1 manager and 2 followers
			Total: 11	5 managers and 6 followers

Ⅳ. Case Contexts

4.1. Three Japanese Case Companies Caught in the 2011 Earthquake

All of the three cases from Japan were concerned the massive 2011 earthquake which was accompanied by a tsunami in the northeastern seaboard and the nuclear accident at the Fukushima nuclear power plant. These companies experienced a variety of challenges, common to which was trouble with the communications network, the electricity cuts, and traffic chaos that followed in the days after the earthquake. All companies had in place a robust and rehearsed system for earthquake safety measures, with assigned duties, floor announcements and evacuation zones. They had prepared plans and task lists for emergencies and set up special control rooms. Therefore, no company of these three was taken entirely unawares by the disaster. None of the companies had their primary activities or core units within the tsunami-hit Tohoku area, and thus none suffered a decimating blow to their operations. Nevertheless, the scale of the disaster was shocking even for these earthquake-hardened Japanese companies.

AUTO has a manufacturing base outside the tsunami-hit northeastern area, and therefore production was not initially affected by the disaster. The company was, however, exposed due to its distribution and supplier network. The first response consisted of an employee report-in and investigation of the damage to the IT network connecting to the local dealers in the Tohoku region. Later, an unexpected contingency unfolded: it was realized that the suppliers of the company had problems in producing specific components upon which hinged the assembly of certain types of car. In other words, the unavailability of just one component might prevent the company in assembling a given car model, and thus stop the value chain for this product. An IT solution was found to be helpful in responding to this problem.

INSURE had its headquarters away from Tohoku area, but several local branch offices and a regional headquarters as well as many local agencies were seriously affected by the disaster. The company was faced with the prospect of considerable insurance payments especially in the area affected by the tsunami, where whole towns had been swept away by the tide. The earthquake had also damaged countless buildings and structures in the Tohoku region. For the IT unit this meant that technical support had to be provided to the local branch offices and agencies that had damaged IT equipment or had lost their data connection to the central information databanks. One emergency measure was to send expert reinforcements to the regional headquarters in the Tohoku area in order to locally administer this technical support. The crisis also served as a valuable lesson to the IT unit in terms of testing the earthquake emergency procedure.

As the two other companies, SERVICE's headquarters were located safely out of the tsunami range. However, in the wake of the disaster, it was found that the company IT systems were vulnerable. International transactions which the Service conducts on a day-to-day basis require access to the foreign exchange systems and this system needed special attention during the communication outages when the earthquake hit. Trouble was also found in the security systems of the company which were supposed to be helpful precisely during this type of crises. For example, confirmation of the safety of employees had to be conducted by a work-around because of this failure.

4.2. Two Taiwanese Case Companies in Two Separate Earthquake Events

The two cases from Taiwan report on two separate earthquake events. Both of these earthquakes were smaller in magnitude than the 2011 earthquake in Japan, and were not accompanied by tsunami. They also resulted in fewer casualties than the huge 2011 event. However, the challenges faced by the IT functions in the two cases presented here are quite similar; they underline problems resulting from both physical damage as well as societal disruption from the earthquakes. Taiwanese companies are accustomed to and prepared for earthquakes due to the frequency that these events strike the island. While the degree of organizational preparedness was different in the two cases, both these companies had prepared plans for crisis situations.

TELECOM was tasked with administering undersea cables in the waters around Taiwan. Earthquakes have the potential to damage these cables, and if this happens, there is a very expensive disruption in telecommunications. To minimize the disruption, the company had set up a specialized team to respond to such damages and take responsibility for the recovery effort. This team had already been functioning for years and had accumulated substantial experience, gradually routinizing their task of earthquake response and recovery. This case focuses on a large earthquake occurring at a time when the team was experimenting with a new IT system developed in-house to assist in communicating with different stakeholders in the response and recovery effort.

In the BANK case, the earthquake caused an emergency that prompted the government to order all businesses to close nationwide for some days. While there had been no damage to BANK IT infrastructure, the closure of offices meant that on-line and telephone customer service for Taiwanese customers abroad had to be organized using an alternative means. The executive management decided to reroute email and call contacts addressed to the Taiwan customer service center to Hong Kong and Singapore, two overseas locations that this BANK had customer service centers. Unfortunately, these two offices were not prepared to serve Taiwanese customers to the extent that they were used to, and IT was part of the problem.

Ⅴ. How Recommendations are Evident in IT Manager Actions During Crisis Response

This section gives examples from the five cases on how the recommendations given to general management on crisis response are evident in the actions of the IT managers. <Table 4> shows how actions were distributed among the six categories of recommendations, with "none" indicating that no action was identified related to the recommendations in that category. However, if actions were identified, only one example action is shown in the table due to lack of space. As can be seen, most examples tell about actions that were according to recommendations, rather than against them.

Each subsection hereafter corresponds to one category of recommendations, and gives a brief description on the actions identified.

5.1. Detecting Problems

Each of the five cases described the identification of critical information during crisis response. Often in these cases, the IT manager became aware of a way that the technical system operates which leads to a problem in the unusual circumstances of the

<Table 4> Examples of Behaviors Identified in the Six Categories

Recommendation	AUTO	INSURE	SERVICE	BANK	TELCO
Detecting problems	Detection of the need for a database following the stock level of crucial parts	Guessing that hands-on IT support would be needed on ground zero	Realization that currency exchange systems needed a human presence	Failure to recognize the lacking customer service capacity of overseas offices	Alertness for incorrect reports and compound disaster damage
Resourcing	none	Certain evacuation details were improvised	none	none	The team maintained a single purpose: rapid recovery of cable damages
Decision-making	The usual procedures for justifying projects were bypassed	Decision-making was conducted in a group of 30-40 managers with constant video link to the HQ	The manager made an exception to the CEO order of having everyone return home from the HQ	An executive team convened to decide on disaster response actions	The manager kept his calm and reassured the staff of success
Coordinating	The manager prefers to focus on the objectives and skip formal communication when delegating tasks	A whiteboard was used to keep track of events and constantly updated with new information	none	The manager had a conference call with executives every day during the service outage	The team tested a new IT system for coordination that reduced the number of telephone calls among stakeholders
Communication	The manager talks in very concrete terms	The number of separate email messages during the crisis was limited	none	none	The team reports to the manager early if problems appear
Emotion management	none	none	none	After the earthquake, the manager called each of his direct staff to make sure they are safe	The manager stayed in the office constantly during the crisis resolution period

crisis response. For example, at AUTO, the unavailability of certain parts due to supply problems caused by the earthquake led to the company being ultimately unable to produce certain car models before the supply problem would be solved. This necessitated that a system be rapidly created to detect the often complex interrelationships between the parts that became unavailable and the car models in which they were used. Another example is a customer service problem at the BANK. A destructive earthquake made company headquarters issue an order to close all offices in the Taiwan branch office, and reroute customer telephone services and electronic services to overseas offices. However, the IT manager soon received customer complaints that these locations were insufficiently prepared to offer service in Mandarin Chinese, and in traditional Chinese characters in the case of written communication. While the IT manager was still in charge of the service for Taiwanese customers, he had no power over the branch offices, and he had no choice but to relay the finding to his superiors for consideration.

5.2. Resourcing

Behaviors related to clarifying roles and resources were identified in two of the cases. On the preparation side, evacuation procedures had been agreed in advance and were familiar to participants at INSURE and SERVICE – which is natural in Japan, a country beset by frequent earthquakes. Even so, it became clear in the INSURE case that preparations were not sufficient. The building housing the IT function was constructed on a plot of land that geological surveys had found to be particularly resistant to earthquakes, and therefore, the possibility of earthquake causing damage to the building had been thought as being minimal. Perhaps because of this, certain details in earthquake-caused evacuation procedures had not been specified or trained for. These included, for example, the nomination of a person with authority to give an order to evacuate, or to determine that the situation is safe and order everyone to return to their workstations. These omissions were realized in the midst of evacuations when the building took structural damage from the quake, despite its assumed safe location.

5.3. Decision-making

IT managers were required to make resolute decisions in most of the case companies because of their technical leadership role. It was particularly poignant that in SERVICE, the IT manager made an on-the-spot exception to the executive command to have all staff return to their homes. He realized that the currency exchange system of the company would have to be exceptionally manned overnight to bring the system to a controlled end state. This made him order that some employees would have to stay at the office to work with the system. At INSURE, the IT manager gave a dangerous task to two of his employees and sent them on a long journey by rental car to the tsunami-hit area to provide technical assistance to the local offices, which had damaged systems. This decision was made in a situation which no one knew the road conditions along the way, the availability of food, and of shelter.

At INSURE and SERVICE, many decisions were made not alone by the IT manager but together with others in a group meeting. At INSURE, the decision-making environment was a “war-room” with about 40 managers present during meetings, both from executive level and middle management. These meetings were held multiple times a day in the beginning of the crisis response, with frequency tapering off at the end of the period. A smaller group of 18 members was present in the meetings of SERVICE, and certain recovery decisions were taken in another meetings together with other executive-level managers.

5.4. Coordinating

Different arrangements were used to share information with all stakeholders during crisis response. The most advanced method of doing so was used by TELCO, which had developed an information system for storing and sharing the status and recovery information regarding damaged telecommunication cables. All stakeholders had access to the system and customized views to the data, which allowed them to access the needed information without repeated contacting to the crisis response team. Others, such as AUTO and INSURE, had prepared dedicated "war-rooms" for crisis response with not only top executives but also important middle management attending. In this space they could use videoconferencing to contact the headquarters, share situational information, and make crucial decisions as the events progressed. The IT manager at INSURE told about a particular method their organization found helpful to follow what was going on. They assigned a team of persons to keep writing the data stream from the field onto a whiteboard day and night, making the whiteboard a constantly updated situational map of the events.

5.5. Communication

The clarity of communication was emphasized in two company cases. At INSURE, conscious attention was focused by the IT manager on communicating with the whole staff of the IT unit. The number of emails sent to employees was limited to avoid confusion and uncertainty, and the source of communications was always the headquarters of the IT unit, avoiding multiple conflicting information sources. On the other hand, at AUTO, the IT manager himself exercised a clear and concrete discussing style while talking with his direct subordinates, which made it easier and quicker for them to catch the gist of what he wanted them to do without lengthy explanations.

5.6. Emotion Management

Several of the IT managers told that they worked long hours during the crisis response. For instance, the IT manager of TELCO said he would focus all his strength on solving the problems during crisis response and would even stay at the office all night if necessary for several days in a row. The IT manager of BANK, on the other hand, told about his immediate intervention on behalf of his employees. He had set a rule that when he called his direct subordinates to establish whether they are safe or not, they would in turn call their subordinates to verify that everyone in his organization was safe. This routine was found to be manageable in the crisis response situation.

Ⅵ. Discussion

While this research did not attempt to establish the value of the crisis response recommendations in IT manager behavior, or the consistency at which these recommendations are followed by IT managers, the results enable the identification of these recommendations for IT managers over a range of company cases in two different countries. This is valuable, because it can help us understand how IT managers behave in crisis response through the lens of previously available "good practice", setting the stage for more comprehensive investigations of IT manager working styles in emergencies, and paving the way for IT manager - focused recommendations in crisis response. The set of recommendations includes categories, specifically "detecting problems" and "decision-making", which were identified for all company cases. Also the individual recommendation of "identification of critical information" was identified for all cases. However, the rest of the recommendations were identified in some but not all cases.

As IT managers are responsible for managing organizational information resources, some of the recommendations can have particular importance for IT managers. For example, IT managers can be expected to be in a position that allows them to be among the first in organizations to detect certain problems that foreshadow crises. They might also be among the first to be alerted to subtle hints that are connected to the escalation of crisis situations. The cases investigated in this research indeed reveal that certain important insights were made by the IT managers. In all cases the insights were connected to the functioning of IT systems. Such kind of insights are difficult to make, however, because they require expert knowledge on the functioning of the systems, the connections between the systems, and the organization, processes, and so on. It may be that only people who are sufficiently technologically adept, yet have a wide, managerial view of systems, are able to make the necessary judgements and predictions on the data available.

Coordination and sharing information are other aspects that would seem to be particularly important for IT managers. Communication channels between stakeholders are often established using IT tools, giving IT managers central roles in any crisis response effort. Accordingly, the IT manager was closely involved in the coordination of the crisis response in most of the case companies of this research. In two of these cases, the coordination involved an IT system that was developed specifically for crisis response, showing that the IT manager's involvement was crucial. While the actual development of these systems often takes place before the crisis, the IT manager may be the only technically oriented person participating in the crisis response team who can give the appropriate direction for the team to use the systems. On the other hand, if such systems have not been prepared, or they prove unworkable, developing ad hoc systems for coordination will be an urgent task for the IT manager. This kind of experiences were reported in the company cases in this research as well.

In contrasting our results to prior research, the resources and actions in crisis response proposed by Leidner et al. (2009) have common ground with the recommendations that were shown as important in this research. For example, the recommendation for identification of critical information is similar to the organizational ability to recognize signals, and the recommendation for sharing information with all stakeholders resembles the action of resolute informing. In particular, Leidner et al. describe how the relief center in Singapore acted as an information hub for other stakeholders in the Asian Tsunami crisis, and that the center's ability to build and apply IT was crucial in this role.

While the acquisition and development of technological tools to assist in crisis response is crucial, the cases show that many activities taken by IT managers are "coping" activities, and that these activities may be well understood by using existing theories in the crisis management literature. Much has been written on improvisation (Pina e Cunha et al., 1999) and bricolage (Ciborra, 1992), and research aiming at elucidating the nature of these concepts in the context of crises would be particularly valuable, because no crisis exactly conforms to previous deliberations.

Finally, and perhaps most importantly, the IT managers stated in their interviews that strong and trusted relationships with the followers are crucially important in crisis response situations. As such relationships cannot be built during crisis response (Boin et al., 2005), the IT manager must take time to build these relationships over long term. Therefore, the preparation for crisis response can be seen as capability building (Leidner et al., 2009) with not only technological and organizational dimensions, but also with human relations dimensions. While the emphasis of this paper has been on actions during crisis response, it should be kept in mind that these actions are based on technological, organizational, and human relations conditions that have been established over a time period before the crisis.

Ⅶ. Contributions, Limitations, and Future Research

This research addresses the behavior of IT managers in crisis situations, a topic which is important because of the vulnerability of IT to disruptions, but also because of IT's crucial role in communications during crisis times. While scholars have investigated CIO leadership in stable situations (Applegate and Elam, 1992; Chen et al., 2010), IT manager behavior in crisis situations has not yet received the attention that it should. This paper answers the call by Pan et al. (2012) to examine individual-level communications and improvisation during crises in the IT function, and reports on an exploratory field investigation that collected data from five companies in Japan and Taiwan on the experiences of IT managers and their subordinates from earthquakes. To appreciate these experiences, recommendations given for organizations during crisis response were applied in the analysis.

The research contributes to theory by identifying several behaviors in IT manager crisis response behavior, that have been prescribed as "good" behaviors in organizations or for the general management during crisis response in crisis management literature. Hence, when examining particularly IT managers as organizational actors, these behaviors stood out from the set of recommendations. They are: "identification of critical information", "clarifying roles and resources", "resolute decision-making", "multiple advocacy decision-making", "sharing information with all stakeholders", "clear communication focusing on essentials", "leader field presence", and "immediate crisis intervention". While different cases emphasize different aspects of crisis response, the behavioral categories of detecting problems and decision-making, as well as the individual behavior of "identification of critical information" were found for all of the cases, suggesting their importance in crisis response for IT managers. This result can serve as a building block to improve the theory of IT manager crisis response in two ways, explained below.

Firstly, it links to the discussion on IT manager and CIO leadership. This research stream harks back to Mintzberg (1973)'s Managerial Roles, where decisional roles such as disturbance handler were identified. Our cases suggest that for IT managers during crisis response, the role of disturbance handler includes a number of important behaviors that are emphasized as society becomes increasingly dependent on technology. Scholars such as Leidner et al. (2009) have shed light on these behaviors in the organizational level, but more research in the spirit of what Chen et al. (2010) have done is necessary to more comprehensively understand how IT managers can be successful in crisis response activities.

Secondly, our research emphasizes that IT manager crisis response consists of not only technical activities, but also human-oriented leadership activities. Therefore, theorizations of IT manager crisis response can be beneficially informed by the leadership field. The behavioral category of detecting problems assumes that IT managers are able to access relevant information rapidly, requiring frank relationships with subordinates. The literature on leadership has developed a wealth of theories that can be applied to understand IT manager leadership in this respect, for instance, the theory of transformational leadership. Such theories should be applied more frequently in research related to IT manager crisis management.

Thirdly, IT manager crisis response behaviors are embedded in the information exchange among individuals, groups, and organizations. The recommendations concur with the star network structure in crisis communication proposed by Pan et al. (2012).

In the star structure, information is exchanged both top-down and bottom-up in the communication network, which is consistent with one recommendation underlined in this paper, that of sharing information with all stakeholders. Pan et al. write that the star structure is dependent on a centralized and trusted crisis response organization which has strong partnerships with other stakeholders and knows the information needs of these stakeholders. It would doubtless be hard to satisfy these requirements without involving the stakeholders by multiple advocacy decision-making and clear communication, which were among the recommendations that were identified in this research. One avenue of future research could be to examine the actions required from the IT managers to create and maintain organizational communication structures for crisis response such as this star network structure.

Although the recommendations appear as good practice in crisis management literature, this research makes no attempt to judge how "good" the recommendations are for IT managers in particular. Therefore, the recommendations should be viewed as a resource which can be used by IT managers to prepare for crisis response, rather than a strict prescription. By applying the recommendations, which come from outside the business continuity management field, the paper challenges IT managers to consider a wide range of crisis response activities that seem to be part of the reality in crisis situations for the IT manager as well. In addition, IT managers can use the cases presented in this paper as inspiration for their own organizations' crisis management preparations.

The research also has some limitations. Our cases were all from earthquakes. Other types of crises may allow the identification of yet more behaviors. As is common in qualitative research, the number of organizations investigated was limited, though we believe that this disadvantage is offset by the amount of data we were able to acquire in the interviews.

In addition to what is written above, future research should add more crisis cases to investigate whether the remainder of the recommendations can be found in IT manager behavior. Furthermore, research is needed to find whether there are IT manager – specific recommendations that were not found with the approach in this paper. Such behaviors are likely to involve more traditional, business continuity management actions. It should be also kept in mind that this research only used the recommendations as a device to understand IT manager behavior in crisis situations, but it did not attempt to judge how good the accompanying behaviors are, nor comprehensively model such behavior. These, too, should be taken as objectives in future research.

Acknowledgements

We acknowledge the financial support of Taiwan Ministry of Foreign Affairs, Canon Foundation, the University of Liege and the European Union in the context of the FP7-PEOPLE-COFUND-BeIPD project, and the 2-Year Research Grant of Pusan National University.

<References>

[1] Andrews, W. C. (1990). Contingency Planning for Physical Disasters. *Journal of Systems Management, 41*(7), 28-32.

[2] Aon Benfield (2012). *2011 Thailand Floods Event Recap Report, Aon Corporation.* Retrieved from http://thoughtleadership.aonbenfield.com/Documents/20

120314_impact_forecasting_thailand_flood_event_recap.pdf

[3] Applegate, L. M. and Elam, J. J. (1992). New Information Systems Leaders: A Changing Role in a Changing World. *MIS Quarterly, 16*(4), 469-490.

[4] Ashir, A. (2014). An Empirical Investigation of Task-Technology Fit: Context of RFID in Disaster Management. *Asia Pacific Journal of Information Systems, 24*(3), 345-370.

[5] Bass, B. M. (1985). *Leadership and performance beyond expectations*. New York, NY, USA: Free Press.

[6] Benjamin, R. I., Dickinson, C., and Rockart, J. F. (1985). Changing Role of the Corporate Information Systems Officer. *MIS Quarterly, 9*(3), 177-188.

[7] Benson, J. A. (1988). Crisis revisited: an analysis of strategies used by Tylenol in the second tampering episode. *Central States Speech Journal, 39*, 4-66.

[8] Boin, A., Paul, H., Stern, E., and Sundelius, B. (2005). *The Politics of Crisis Management: Public Leadership Under Pressure*. Cambridge, UK: Cambridge University Press.

[9] Calloway, L. J., and Keen, P. G. W. (1996). Organizing for Crisis Response. *Journal of Information Technology, 11*, 13-26.

[10] Chen, D. Q., Preston, D. S., and Xia, W. (2010). Antecedents and Effects of CIO Supply-Side and Demand-Side Leadership: A Staged Maturity Model. *Journal of Management Information Systems, 27*(1), 231-271.

[11] Ciborra, C. U. (1992). From Thinking to tinkering: The grassroots of IT and strategy. *Information Society, 8*, 297-309.

[12] Cohen, M. J. (2003). State-level Emergency Response to the September 11 Incidents: the Role of New Jersey's Department of Environmental Protection. *Journal of Contingencies and Crisis Management, 11*(2), 78-85.

[13] Comfort, L. K., and Haase, T. W. (2006). Communication, Coherence and Collective Action: The Impact of Hurricane Katrina on Communications Infrastructure. *Public Works Management and Policy, 10*(4), 328-343.

[14] Comfort, L. K., Ko, K., and Zagorecki, A. (2004). Coordination in Rapidly Evolving Disaster Response Systems: The Role of Information. *American Behavioral Scientist, 48*(3), 295-313.

[15] Comfort, L. K., Siciliano, M. D., and Okada, A. (2011). Resilience, Entropy, and Efficiency in Crisis Management : The January 12, 2010, Haiti Earthquake. *Risk, Hazards & Crisis in Public Policy, 2*(3), 1-25.

[16] Coombs, T. (2007). *Ongoing crisis communication: planning, managing and responding*. Los Angeles, USA: Sage.

[17] Day, J. M., Junglas, I., and Silva, L. (2009). Information Flow Impediments in Disaster Relief Supply Chains. *Journal of the Association for Information Systems, 10*(8), 637-660.

[18] Devadoss, P. R., and Pan, S. L. (2004). Leveraging e-Government Infrastructure for Crisis Management: Lessons From Managing SARS Outbreak in Singapore. *Journal of Information Technology Theory and Application, 6*(3), 25-40.

[19] Devitt, K. R., and Borodzicz, E. P. (2008). Interwoven Leadership: The Missing Link in Multi-Agency Major Incident Response. *Journal of Contingencies and Crisis Management, 16*(4), 208-216.

[20] Drabek, T. E., and McEntire, D. A. (2003). Emergent phenomena and the sociology of disaster: Lessons, trends and opportunities from the research literature. *Disaster Prevention and Management, 12*(2), 97-112.

[21] Drennan, L. T., Stark, A., and McConnell, A. (2015). *Risk and Crisis Management in the Public Sector*. London, UK: Routledge.

[22] Dubé, L., and Paré, G. (2003). Rigor in Information Systems Positivist Case Research: Current Practices, Trends, and Recommendations. *MIS Quarterly, 27*(4), 597-636.

[23] George, A. L., and Stern, E. K. (2002). Harnessing conflict in foreign policy making: from devil's to multiple advocacy. *Presidential Studies Quarterly, 32*, 484-508.

[24] Hankyoreh (2018). *Disaster at S. Korean*

telecommunications giant exposes weakness of ‘superconnected’ society. Hankyoreh, November 26, 2018. Retrieved from http://english.hani.co.kr/arti/english_edition/e_national/871848.html

[25] Harnesk, D. (2013). Collective IT Artifacts: Toward Inclusive Crisis Infrastructures. *Journal of Information Technology Theory and Application, 14*(4), 27-48.

[26] Hecht, J. A. (2002). Business Continuity Management. *Communications of the Association for Information Systems, 8*, 443-451.

[27] Herbane, B., Elliott, D., and Swartz, E. M. (2004). Business continuity management: Time for a strategic role? *Long Range Planning, 37*(5), 435-457.

[28] House, R. J., Hanges, P. J., Javidan, M., Dorfman, P.W., and Gupta, V. (eds.) (2004). *Culture, Leadership, and Organizations: The GLOBE Study of 62 Societies*. Thousand Oaks, CA, USA: Sage.

[29] Housel, T. J., El Sawy, O. A., and Donovan, P. F. (1986). Information Systems for Crisis Management: Lessons from Southern California Edison. *MIS Quarterly, 10*(4), 389-400.

[30] Ives, B., and Olson, M. H. (1981). Manager or technician? The nature of the information systems manager's job. *MIS Quarterly, 5*(4), 49-63.

[31] Janis, I. L. (1982). *Groupthink*. Boston, USA: Houghton Mifflin.

[32] Jennex, M. E. (2004). Emergency Response Systems: The Utility Y2K Experience. *Journal of Information Technology Theory and Application, 6*(3), 85-102.

[33] Kawamura, M. (2012). BCPからみた東日本大震災とタイ大洪水の教訓. *Nippon Life Insurance Research Institute*. Available at: https://www.nli-research.co.jp/files/topics/39783_ext_18_0.pdf

[34] The Korea Herald (2018). KT chairman apologizes for chaos, scrambles to contain damage from fire. *The Korea Herald*, November 25, 2018. Retrieved from http://www.koreaherald.com/view.php?ud=20181125000202

[35] The Korea Herald (2018). KT's mobile phone subscribers down after fire disrupts services. *The Korea Herald*, November 27, 2018. Retrieved from http://www.koreaherald.com/view.php?ud=20181127000663

[36] Kotter, J. P. (1988). *The Leadership Factor*. New York, USA: Free Press.

[37] Leidner, D. E., Pan, G., and Pan, S. L. (2009). The role of IT in crisis response: Lessons from the SARS and Asian Tsunami disasters. *Journal of Strategic Information Systems, 18*, 80-99.

[38] Lettieri, E., Masella, C., and Radaelli, G. (2009). ”Disaster management: findings from a systematic review. *Disaster Prevention and Management, 18*(2), 117-136.

[39] Lewis, G. (2006). *Organizational Crisis Management: The Human Factor*. Boca Raton, FL, USA: Taylor & Francis.

[40] McKinney, E. H. (2008). Supporting Pre-existing Teams in Crisis with IT: A Preliminary Organizational-Team Collaboration Network. *Journal of Information Technology Theory and Application, 9*(3), 39-59.

[41] Mintzberg, H. (1973). *The Nature of Managerial Work*. New York, NY, USA: Harper & Row.

[42] Northouse, P. G. (2007). *Leadership: Theory and Practice*. Thousand Oaks, CA, USA: Sage.

[43] Pan, S. L., Pan, G., and Leidner, D. E. (2012). Crisis Response Information Networks. *Journal of the Association for Information Systems, 13*(1), 31-56.

[44] Pee, L. G., and Lee, J. (2016). Trust in User-Generated Information on Social Media During Crises: An Elaboration Likelihood Perspective. *Asia Pacific Journal of Information Systems, 26*(1), 1-21.

[45] Perrow, C. (2007). *The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters*. Princeton, NJ, USA: Princeton University Press.

[46] Pina e Cunha, M., Vieira da Cunha, J., and Kamoche, K. (1999). Organizational Improvisation: What, When, How and Why. *International Journal of Management Reviews, 1*(3), 299-341.

[47] Quarantelli, E. L. (1997). Ten Criteria for Evaluating the Management of Community Disasters. *Disasters, 21*(1), 39-56.

[48] Smaltz, D. H., Sambamurthy, V., and Agarwal, R. (2006). The antecedents of CIO role effectiveness

in Organizations: An empirical study in the healthcare sector. *IEEE Transactions on Engineering Management, 53*(2), 207-222.

[49] Stephens, C. S., Ledbetter, W. N., Mitra, A., and Ford, F. N. (1992). Executive or Functional Manager? The Nature of the CIO's Job. *MIS Quarterly, 16*(4), 449-467.

[50] Strauss, A., and Corbin, J. (1990). *Basics of Qualitative Research*. Newbury Park, USA: Sage.

[51] Thomas, M, A., Andoh-Baidoo, F. K., Redmond, R., and Yoon, V. Y. (2009). Moving Beyond Traditional Emergency Response Notification with VoiceXML. *Journal of Information Technology Theory and Application, 10*(1), 28-40.

[52] Turoff, M. (2002). Past and Future Emergency Response Information Systems. *Communications of the ACM, 45*(4), 29-33.

[53] Ulmer, R. R., Sellnow, T. L, and Seeger, M. W. (2007). *Effective Crisis Communication: Moving from Crisis to Opportunity*. Thousand Oaks, CA, USA: Sage.

[54] Wang, W. T., and Belardo, S. (2009). The Role of Knowledge Management in Achieving Effective Crisis Management: A Case Study. *Journal of Information Science, 35*(6), 635-659.

[55] Weick, K. E. (1988). Enacted sense making in crisis situations. *Journal of Management Studies, 25*(4), 305-317.

[56] Weick, K. E. (1990). The vulnerable system: An analysis of the Tenerife air disaster. *Journal of Management, 16*, 571-593.

[57] Wu, J. H., Chen, Y. C., and Lin, H. H. (2004). Developing a Set of Management Needs for IS Managers: A Study of Necessary Managerial Activities and Skills. *Information & Management, 41*, 413-429.

[58] Xue, Y. J., and Liang, H. G. (2004). IS-Driven Process Re-engineering: China’s Public Health Emergency Response to the SARS Crisis. *Journal of Information Technology Theory and Application, 6*(3), 41-58.

[59] Yin, R. (2009). *Case Study Research: Design and Methods*. Beverly Hills, CA, USA: Sage.

◆ About the Authors ◆

Tommi Tapanainen

Tommi Tapanainen is Assistant Professor at the Department of Global Studies at Pusan National University. His research interests are in IT incident and crisis management and IS agility.

Olivier Lisein

Olivier Lisein is Assistant Professor at HEC Management School – University of Liège and Senior Research Associate at LENTIC – University of Liège. His research interests are related to digitization, change/innovation management, and organization theory.

Ryuichi Hosoya

Ryuichi Hosoya is a Ph.D. candidate at the Graduate School of Commerce and Management, Hitotsubashi University. His research interest is in the process through which information systems diffuse and assimilate in organizations. His PhD study focuses on how different types of big data analytics use contribute to firm's agility through sensemaking of data being analyzed.

Taro Kamioka

Taro Kamioka is Professor at the Graduate School of Business Administration, Hitotsubashi University. His research interests are the roles of Chief Digital Officers, and Big Data Analytics.

Submitted: November 13, 2018; 1st Revision: January 18, 2019; Accepted: March 1, 2019