2-2012

The central role of information systems in managing crises

Knowledge@SMU

(http://knowledge.smu.edu.sg)

The central role of information systems in managing crises

Published: February 16, 2012 in Knowledge@SMU

Crisis management research recognises the importance of timely information in coordinating a suitable and rapid crisis response. However, the transmission of information would depend on the information systems assets available, how they work with other resources and how they facilitate coordination – areas that have not received much scholarly attention.

In '*The Role of IT in Crisis Response: Lessons from the SARS and Asian Tsunami Disasters*', Dorothy E. Leidner (http://business.baylor.edu/Dorothy_Leidner/) (Baylor University), Gary Pan (http://www.accountancy.smu.edu.sg/faculty/accounting/garypan.asp) (Singapore Management University), and Shan L. Pan (http://www.comp.nus.edu.sg/~pansl/) (National University of Singapore) studied the mechanisms through which information systems aids crisis response and the preconditions for its effective use. The paper was published in the 18th edition of the *Journal of Strategic Information Systems*.

As societal and economic crises typically involve cooperation and coordination between several public and private organisations, "information collecting, synthesising, interpreting, and communicating across the multiple organisations becomes a central challenge," the researchers wrote. A failure to address these challenges will lead to costly delays in resolving the crises at hand.

Decision makers also require information before they can choose which actions to take. To speed up their responses, communication channels may be reduced, but this risks the passing over of potentially critical data. Effective crisis response thus requires weighing between the need to act and the need to collect and process information.

To examine these interactions along the information systems value chain, the authors adopted a resource-based view (RBV). This theoretical lens, they argued, would offer a better understanding of those critical response characteristics, and enable a deeper appreciation of information systems' roles within the larger ecosystem of complementary resources.

While the theory has traditionally been applied with *competitive*, as opposed to *cooperative* studies, the authors explained that RBV would be relevant to their research because it is – as the theory was intended – an organisation-level study of resources and capabilities in driving performance.

"By extending RBV to a cooperative environment, we remain true to the implicit goal of understanding performance, but rather than understanding why one firm outperforms others, we are interested in how a constellation of firms cooperating may perform effectively," they wrote.

Having laid down their research goals – (1) to understand which information systems resources are most valuable in crisis response situations, (2) how they may be bundled with other resources for synergy, and (3) how such resources are coordinated across organisations – the authors zeroed in on two past major incidences for answers.

The first incidence was 2003's outbreak of the highly infectious Severe Acute Respiratory Syndrome (SARS) that led to national health crisis, and the second, 2004's Asian Tsunami, where Singapore played a regional relief-coordination role.

A hybrid research method that included qualitative case studies and semi-structured interviews with the 23 relevant members and executives was employed. Media coverage of the events served as secondary data, along with official press releases, internal documents and discussion notes.

Case 1: Managing a health crisis

When SARS broke out in March 2003, Singapore's Ministry of Health (MOH) set up a nine-member high-level ministerial task force. Contact tracing of SARS patients was initiated to identify the places a patient had visited so as to subsequently locate people who had also visited the same places. This effort required the involvement of other ministries, and so several statutory boards were roped in.

MOH had then requested that the Defence Science and Technology Agency (DSTA), a statutory board under Singapore's Ministry of Defence, set up an operations centre for contact tracing. DSTA, with its prior experiences in national IT projects, proceeded to build a centre with capabilities for large-scale contact tracing and data management.

IT applications were developed to keep track of relevant healthcare professionals, patients, their contacts, and at the same time, plot linkages between each person. DSTA had also developed a Case Management System (CMS) to facilitate data exchanges across government agencies. At airports, prototype infrared fever screening systems (modelled after military-grade thermal imagers) were installed and those suspected of carrying the disease would receive on-site medical attention.

After the crisis had bowed out, Singapore was praised for its efficiency in "managing the spread of SARS and minimising the damage". However, the authors noted that there was some unhappiness over the "hyper-response" and "overkill" approach to the crisis. There were also privacy concerns over the use of scanners and sharing of patient data.

Case 2: Coordinating relief

Following the Asian Tsunami disaster on Boxing Day 2004, DSTA was tasked to set up the Singapore Regional Coordination Centre's (SRCC) IT infrastructure. It was during this time that they rolled out the web-based Crisis Case Management System (CCMS) – an application that could manage the distribution of aid supplies, track manpower deployment and movement, and at the same time, facilitate communication.

By January 2005, about 20 non-governmental organisations (NGO) had started their operations at the SRCC. The Singapore Armed Forces (SAF) provided supporting services to the SRCC which included coordinating public donations, updating spreadsheets, packing and shipping of aid supplies, as well as performing matches between aid demand and supply.

The SAF had, additionally, set up other operations centres to coordinate additional relief activities, such as the updating of tsunami information and aid delivery schedules. This involved frequent communications between the Singapore-based officers and on-site workers from the Thai and Indonesian military.

It was inevitable that kinks would show up within complex coordination initiatives as such. Despite frequent information updates from the SRCC, the authors revealed that distribution problems and overcrowding had, at one point, caused tons of emergency medical and food supplies to be stuck at the airport.

There were also issues with the oversupply of some relief items and the undersupply of others. An informant commented, "While we could take heart that there was a strong response to the tremendous humanitarian needs, there was a need for a more systematic, streamlined and efficient approach to private sector participation in humanitarian work. Perhaps an infrastructure for private sector for partnership could be created and prepared for the next crisis."

Technology uses and users

By most accounts, it was agreed that a "strong and flexible" IT infrastructure would be vital in the management of crises. They are especially useful "where disparate organisations need to coordinate information," the authors observed from both case studies.

Relating their findings to the RBV, the authors noted that while the "mobile and imitable" skills of information systems experts may be considered to be of lower value within competitive environments, they were "essential" in the cooperative context of crises as these very skills bolstered speed and agility.

Next, they pointed out that the value of information systems resources increases as assets and capabilities are, synergistically, bundled together. As an example, they suggested that professional skills, when applied with an understanding of the context and culture, present a far greater advantage to management. Indeed, the extensive network of relationships at DSTA had facilitated the rapid development and implementation of the crisis information system in both cases.

The value of collaborative networks aside, it is worth noting too, the relationship between IT capabilities and leadership: "Having leadership that was willing and able to recognise the signals early and see the big picture, enabled the IT staff to begin development of crisis response systems early in the crisis, which facilitated the process of resolute informing, gaining stakeholder commitment, and agile mobilising," the authors explained.

The longer decision makers searched for the most optimal solution, the larger the risk that events might spiral beyond control. Failure to recognise the signs could lead to an exacerbation of the crisis. A command structure linking assets and capabilities with adequate response is thus crucial to success.

Both IT and organisational structures should complement each other, they said. In both crises, the top-down centralised command and control enhanced the mobilisation of people and technology, improving the "overall efficiency and interoperability of deployment and distribution-related activities".

Looking ahead, the framework of resource deployment during crisis response as suggested by the central role of IS resources might serve as a "means to evaluate crisis preparedness in organisations and as a springboard to further research into intra as well as inter-crisis learning," the authors concluded.

back to top (#top)

back to top (#top)