

the business continuity
JOURNAL

SEPTEMBER 11, 2001 IN RETROSPECT

A DECADE ON, WHAT BUSINESS CONTINUITY
AND INFORMATION SECURITY LESSONS HAVE
BEEN LEARNED?

By Thomas Virgona, Ph.D

ABSTRACT: This paper describes research which investigated the impacts of September 11, 2001, on information security and looks at how effective disaster recovery and business continuity prepared to protect information systems were. Despite it being almost a decade since the events reviewed in this paper occurred, many of the lessons are not only current, but have not yet been effectively explored or considered.

The research examined the impact on information systems security on the disaster recovery effort associated with September 11, 2001. Specific areas considered included:

- What happened to the systems that day and how did information systems technologists react?
- What changes to the SDLC (specifically humans' role in disaster recovery design planning) have been implemented since September 11, 2001?
- What lessons were learned?

The expected outcome of the research will be a better understanding of issues facing information security during major disasters.

Specific findings included:

- One of the major shortcomings in the disaster recovery or continuity of business design was the reliance on humans to ensure that company's information infrastructure was restored to an operational status.
- Organizations often create elaborate emergency operations plans, but they fail to develop the capability to implement these plans. Disaster plans are important, but they are not enough by themselves to assure preparedness. They can be an illusion of preparedness.
- Informally developed teams are more effective than formal teams.
- Information policies can't be stopped during a crisis, but they need to be relaxed. Due to the human elements and personal relationships, firms need to realize that information system will be changes in an un-controlled manner during a disaster. How these changes conflict with existing information security and change control policies presents an issue for firms.

Author



Dr. Thomas Virgona, Pace University, New York. Tom was an employee at CitiGroup on Wall Street from 1990 to 2009. As a vice president in the technology group, some of his responsibilities included technology information security officer, software quality manager, export licensing and project management. Tom is an associate professor at Central Connecticut State University in the School of Business, an adjunct professor at Pace University in New York City in the School of Computer Science and Information Systems and an adjunct professor at

Westwood (online).

Background

The present time could be characterized as the era of the Internet. Information technology is the present-day equivalent of electricity in the industrial era. The Internet is the fabric of our lives, a ubiquitous presence.

The Internet seems to have some positive effect on social interaction, and it tends to increase exposure to other sources of information. The Internet provides a tool to give a voice to people who would otherwise find difficulty in obtaining that voice. However, the Internet still has difficulty in attracting the most deprived and socially excluded in society. It is in these respects that the Internet, rather than providing a vehicle for liberation, serves to reinforce the prevailing control, as the more powerful have the louder and more eloquent voices (Conway et al 2003). Indeed, wider access and participation in the information society is paramount for broader issues of social inclusion. Many theorists reject any suggestion that the 'information revolution' has overturned everything that went before. On the contrary, they come to explain that it is a primarily an outcome and expression of established and continuing relations (Webster 1995). Herbert Schiller suggests that the information explosion of the post-war years is the consequence, for the most part, of corporate capitalism's inexorable march (Webster 1995).

The Internet is not just a technology, but a technology of freedom. The fundamental digital divide is not measured by the number of connections to the Internet, but by the consequences of both connection and lack of connection (Castells 2003). Technology is a vitally important aspect of the human condition. Technologies feed, clothe, and provide shelter for us; they transport, entertain, and heal us; they provide the bases of wealth and of leisure; they also pollute and kill (Mackenzie and Wajcman 1999). Castells defined the digital divide by the following categories: Income, Education, Age and Ethnic.

The underlying issue of this research is that on September 11, 2001, the terrorist attacks that struck downtown Manhattan rendered Wall Street area financial services unable to provide critical information services. This research will investigate the role information security played during the

recovery efforts following the tragic events following that day. It is important to remember that many of the system failures and outages that occurred on that fateful day are not public knowledge and are treated as confidential information. Despite it being almost a decade since the events reviewed in this paper occurred, many of the lessons are not only current, but have not yet been effectively explored or considered. This paper seeks to highlight some of these areas.

Social scientists generally agree on what disasters are and how they are distinguished from other social phenomena (Kreps, and Kroll-Smith/Gunter in Quarantelli 1998). For this study of September 11, 2001, the Porfiriev definition is sufficient (in Quarantelli 1998). A disaster is a condition destabilizing the social system that manifests itself in a malfunctioning or disruption of connections and communications of a social unit, partial or total destruction, making it necessary to take extraordinary or emergency countermeasures to reestablish stability (Kreps, and Kroll-Smith/Gunter in Quarantelli 1998).

Gilbert classifies disasters into three paradigms (Quarantelli 1998). The first is a catastrophe imputed by an external agent or human communities reacting against an aggression. Gilbert calls this a duplication of war. The second disaster is an expression of social vulnerabilities. The third disaster is an entrance into a state of uncertainty. September 11, 2001 would fall into the first paradigm – duplication of war. These events involve considerable harm to the physical and social environment. They happened suddenly and something might have been done to mitigate their effect before or after they happened (Kreps in Quarantelli 1998).

One of the most visible disruptions was that the New York Stock Exchange (NYSE) ceased all operations for four business days. Although not a direct target of the attack, the dependency on other financial systems (e.g., inter-bank payments and the Federal Reserve Bank) made normal business operations impossible. However, at the core of the issue was the disruption of inter-bank payment systems (Lacker 2003). On that Wednesday (9/12/2001),

Richard A. Grasso, chairman of the New York Stock Exchange, vowed that US stock trading would resume no later than Monday (9/17/2001) (Blustein and Day 2001). The decision to shut down the NYSE and when to return to operation was a difficult one, fraught with risk. There was a risk of bringing the markets back too soon if too few participants were functioning again. Also poor liquidity could hamper trading and exacerbate the expected price declines. Moreover, physical conditions in Lower Manhattan were unpleasant and potentially harmful. Conversely, the symbolic value of a return to normalcy was very attractive.

From an economic and operational perspective, the banking system was in relatively healthy condition on September 11, 2001. From a geographical perspective, it was a true disaster. The facilities of the New York Board of Trade in Four World Trade Center were destroyed. Several firms, including the Federal Reserve Bank itself, were forced to relocate to disaster recovery sites. Regional stock exchanges, the NASDAQ Stock Market, the Chicago Board of Trade, the Bond Market Association and the Chicago Mercantile Exchange all closed as well. European markets remained officially open but from a 'human' perspective, traders found it difficult to do much business. Connections to the Bank of New York (BoNY) were lost for part of the week and as a result the bank

did not know what securities and cash it had received, and it was unable to transmit settlement instructions (Costa 2001).

On the Federal Reserve's Fedwire Funds Transfer System, payments are initiated by the sender of funds, but the major banks' inability to send funds transfer payment instructions following the September 11, 2001 attacks meant funds accumulated in that bank's account. At one point during the week after September 11, BoNY publicly reported to be overdue on \$100 billion in payments (Beckett and Sapsford 2001). The Moscow International Currency Exchange (MICEX), which used BoNY as a business partner, suspended trading due to BoNY's problems.

The events of September 11, 2001 literally struck at the heart of America's financial information center. What impact did September 11, 2001 have on information systems and technology, specifically disaster recovery planning and the role of information security? Scholars believe these 'human' factors present one of the most unpredictable areas for disaster recovery researchers (Sikich 2003). How will humans react to unfolding events? Sikich also puts forth the definition of human factors in the context of business continuity (Sikich 2003). Information security questions that are now relevant include:

- How well do you know your workforce?
- What is the extent of background checks that are part of the screening process?
- Can someone, either overtly, clandestinely, or unwittingly, be compromised into creating an exposure that puts the firm at risk?
- How can you implement checks and balances so that critical information is not subject to compromise?

Control of information has always been dictated by technology. Frederick Ferre stated that the definition of technology is the practical implementations of intelligence (Ferre 1988). There is a tendency to forget that sermons used to couple news, real estate transactions and other mundane matters (Eisenstein 1979). The Sunday paper has replaced church going as an information source. Until Gutenberg, the church had censored ideas more than texts. In the big cities, newspapers succeeded in reaching the general population, whose cultural and educational level was low (Martin 1994). The printing press was such a major technological advancement that Sir Francis Bacon said it was one of the three inventions (printing, gunpowder, and the compass) that changed the state of the whole world (Eisenstein 1979).

The expected outcome of the research described in this paper will be a better understanding of issues facing information security during such disasters. As Gray and Altmann wrote in 2001, information in the world is useful only if we can find it when we need it.

Today, the focus of many governments has shifted to terrorism. Modern disasters are complex enough to require the utmost flexibility in their management. From the 1970s onwards, disaster research stressed non-military models of civil protection, such as the incident command system (ICS). Civil protection later emerged as demand increased under the duress of more serious, civilian disasters such as earthquakes, hurricanes, floods, and transportation crashes (Blanchard 1984). The ICS is different from the traditional command-and-control model derived from the direction of

troops during combat, as it relies on information sharing and collaboration among task forces (Irwin, 1989). Decision making is a major problem in disasters. Other areas for concern during disasters include bureaucratic politics/procedures, groupthink and misperception (McEntire 2004).

From a pragmatic point of view, the traditional System Development Life Cycle is one of the most critical methodologies in information technology. Disaster recovery is dependent on the SDLC for ensuring disaster recovery planning is integrated throughout the technology development process: the requirements for the system's recovery are defined in the analysis phase, the system is designed to provide service during a disaster within the specified timeframes and testing the recovery capabilities is part of the creation of the project, thus ensuring continued use during a disaster.

Despite the evolution and advances in information systems and technology, it is an almost universal finding in studies investigating human information behavior that people choose other people as their preferred source of information (Johnson 2004). Studies of academic researchers in both the sciences and the humanities have revealed the importance of consulting with colleagues at different stages of their research (Johnson 2004). Professionals, such as engineers, nurses, physicians and dentists rely on co-workers and knowledgeable colleagues in their search for work-related information (Leckie, et al., 1996). People are also among the most important sources consulted by chief executive officers during their environmental scanning (Choo 1993). Studies of ordinary citizens' preferred sources of information also confirm the importance of personal contacts in information seeking behavior (Warner 1993). The poor, as well, prefer people over other sources of information (Agada 1999). The explanation for the use of people as information sources has often been that they are "typically easier and more readily accessible than the most authoritative printed sources" (Case 2002). Immigrants are generally perceived to be information poor, meaning they face major challenges with finding and using greatly needed everyday information (Agada 1999). Research findings suggest that personal networks were used more readily than any other type of information source (Fisher 2004). The ability of these populations to establish themselves independently is limited and often restricted by barriers of language and influence. There is a negative spiral effect for these populations as they work to improve their socio-economic situation while being unable to operate outside of the community information system they have established for themselves (Fisher 2004).

Humans have deployed technology to combat disaster since the beginning of recorded history. The cradle of Western civilization, the Tigris-Euphrates river valley, was settled and urbanized through an extensive flood control infrastructure that stabilized the flow of water to fields while also protecting fixed settlements (Moss and Townsend 2006). Over the past century, the role of technology has expanded from just mitigating the impacts of natural disaster to producing disaster itself. The devastating effects of aerial bombardment of cities during 20th century may well have killed more people than all natural disasters in history combined. Chernobyl (1986) and Bhopal (1984) demonstrate the potential for chemical and nuclear industrial accidents to cause major disasters (Moss and Townsend 2006).

A disaster is an unexpected occurrence inflicting widespread destruction and distress and having long-term adverse effects on society. An emergency is a situation or occurrence of a serious nature,

developing suddenly and unexpectedly, and demanding immediate action (power failure and minor flooding) (Hunter 1997). The events of September 11, 2001 can be defined as both an emergency and a disaster.

Following the 1993 bombing of the World Trade Center (WTC), terrorism and security experts agreed that the US financial services industry was a prime target for future terrorist attacks. Experts warned that the financial industry's disaster recovery plans were out-of-date, designed primarily to withstand natural disasters, and were no match for the destructive power of an intentional terrorist attack (Beacham and McManus 2004). Sikich believes one underlying vulnerability issue for organizations continues to be the assumption that threat, hazard, risk, and consequence-assessment are one and the same. These elements are intertwined but are distinct and different (Sikich 2003).

While the tragic events of September 11, 2001 confirmed experts' foreboding predictions of attacks on the US financial system, was the financial services industry inadequately prepared to recover from such an attack? As the financial services sector, and the securities industry in particular, were heavily concentrated within the World Trade Center towers, several such firms emerged as those 'hardest hit' by the September 11, 2001 attack (Cantor Fitzgerald; Keefe, Bruyette & Woods; and Sandler O'Neill & Partners). While the financial services industry as a whole made great strides in recovery and continuity planning regarding data and data systems, the attack on September 11, 2001 revealed inconsistency in the level of disaster recovery preparedness at individual companies. While Cantor Fitzgerald had duplicate systems in place so that its data system never went down, smaller companies, like Sandler O'Neill were less prepared, and had to rebuild their IT system from scratch. What the attack on September 11, 2001 made tragically apparent, however, was the industry's grossly inadequate preparation for the tremendous loss of human capital. While existing recovery plans assumed the safety of company personnel, on September 11, 2001 several companies literally lost their entire disaster recovery team. The bottom line is that the attack on the World Trade Center exposed both the financial services industry's reliance on human capital and its inadequate preparation to recover from such a loss (Beacham and McManus 2004). Johnston and Nedeleescu (2006) wrote that the economic consequences can be largely broken down into short-term direct effects; medium-term confidence effects and longer-term productivity effects. The direct economic costs of terrorism, including the destruction of life and property, responses to the emergency, restoration of the systems and the infrastructure affected, and the provision of temporary living assistance, are in the short run. The medium-term impact is the indirect costs to affect the economy by undermining consumer and investor confidence. Over the longer term, there is a question of whether the attacks can have a negative impact on productivity by raising the costs of transactions through increased security measures, higher insurance premiums, and the increased costs of financial and other counterterrorism regulations.

Connell (2001) discussed the lessons learned from the 1993 World Trade Center terrorist attacks and the impact on the September 11, 2001 event. Panic was not widely observed during the evacuation of the Twin Towers, as the evacuation experiences of many of the workers in the buildings in the 1993 attack may have had an impact on their decision-making process during the September 11 disaster. Improvements made following the 1993 World Trade Center attack contributed to a more successful evacuation. These improvements included the addition of battery-powered lights and

glow-in-the-dark paint in the stairwells, the appointment of floor marshals to guide the evacuation process, and redesigned emergency plans (Connell 2001). Many survivors cited the improved conditions in the stairwells during the September 11 evacuation. As one survivor observed, despite the magnitude of the terrorist attacks on the WTC, the evacuation process did not seem as dire as the evacuation following the 1993 attack due to the improvements in ventilation and lighting. Many organizations located within the WTC significantly improved their evacuation plans following the 1993 terrorist bombing. Individuals were more likely to decide to evacuate the premises if they experienced visual or sensory clues that suggested the dangerous nature of the event. Examples of visual or sensory clues that were cited by survivors in their accounts included smoke, fire, water from the sprinkler systems, debris, structural failure, shattered glass, and the impact of the plane collision (Connell 2001).

Over the past decades, information technology has become increasingly integrated into the day-to-day operations of most financial service organizations. A common phrase today is 'ubiquitous' computing. The dependability and continuity of information infrastructures can be a determining factor in how well an organization will be able to respond to a catastrophic event. Although many lessons can be identified, they emphasize three general principles: the establishment and practice of comprehensive continuity and recovery plans, the decentralization of operations, and the development of system redundancies to eliminate single points of weakness (Seifert 2002).

The events of September 11, 2001 also highlighted an increased need for information technology security not only for New York/Washington business end federal executives, but for other state government executives as well. This increased urgency and heightened awareness left many of Virginia's government executives asking the question, "How secure and prepared is the Commonwealth to deal with information security attacks" (Redwine 2002). Even more alarming is that in 1993, the World Trade Center was the primary target for another terrorist attack. Yet, many organizations were still unprepared.

Business continuity and disaster recovery have become a higher priority for financial services firms in the years since September 11, 2001. Terrorist threats pushed-up global institutions' projected IT spending on operational recovery. The industry closed operational gaps since the destruction of September 11, 2001. These deficiencies included serious weaknesses in business continuity plans, including the need for geographic dispersion of offices, employees and business processes, as well as redundancy of supporting infrastructure, like telecommunications networks and power supplies. Money has been spent on backup systems, storage units, and remote-mirroring technologies. Many have set up remote-workforce operational-resilience plans to ensure that work can be done at satellite offices and other sites (Krebsbach 2004). Oz researched firms directly impacted by the terrorist attacks (Oz 2003). The impact of not having a disaster recovery plan is clear: two of the four companies that did not have a business continuity plan did not regain their business potential.

Research

The research which this paper describes examined the impact on information systems security on the disaster recovery effort associated with September 11, 2001. Specific areas considered included:

- What happened to the systems that day and how did information systems technologists react?
- What changes to the SDLC (specifically humans' role in disaster recovery design planning) have been implemented since September 11, 2001?
- What lessons were learned?

The research has indicated that one of the major shortcomings in the disaster recovery (DR) or continuity of business (COB) design was the reliance on humans to ensure that company's information infrastructure was restored to an operational status. Subsequently, when people could not be located, or in some cases, entire DR/COB departments were killed, restoration of these services failed. Much of the information about the extent of the disaster is still not in the public domain. Oz, in a previous study found four major reasons for this situation (Oz 2003):

- The organization has a policy not to participate in any research survey.
- The organization considers the data confidential despite confidentiality guarantees.
- There is a lack of time to fill out the questionnaire.
- The data is not available.

The purpose of this research is to identify if there was a failure to follow information security procedures that day. Kenneth Hewitt has studied disasters in recent years and has found the most important insights come from the workers on the ground (Quarantelli 1998). Specifically, the most knowledge comes from those on the front-line of a disaster reflecting upon field conditions. Those who speak the language and have some depth of knowledge of the culture provide essential insight (Quarantelli 1998). The methodological challenge of disaster recovery studies is to pay attention not just to the local conditions, but to the voices of the persons involved. Robert Stallings described the challenge of researching disasters: there are many empirical studies, but less certainty as to what they add up to (Quarantelli 1998). This research intends to explore the September 11, 2001 disaster recovery events on Wall Street and identify any patterns observed.

Research methods are varied and have inherent benefits and risks. For this research, non-experimental design was used. Specifically, qualitative analysis techniques were used – exploratory and descriptive. The research goal was to uncover what we have learned from the events of September 11, 2001.

For this reason,

- A focus group data gathering technique was selected.
- The second qualitative technique used for this research was unstructured interviews.
- The third qualitative technique utilized was observation. The researcher observed an actual disaster recovery test conducted by Wall Street financial firms.
- The fourth and final qualitative technique utilized was artifact analysis. Disaster recovery plans from the year 2000 were compared to current disaster recovery plans.

One of the main purposes of this study was to explore empirical data that would help in understanding the information security challenges during a disaster recovery. The present study investigates below the general planning level and identifies the link between technology recovery and the human action required to achieve that task. Though exploratory and descriptive in nature, this research can be used a starting point for further technology studies that focus on providing information services during a disaster.

This study also identifies where knowledge should be captured, which isn't currently being done so. People tend to accumulate information and knowledge informally and may not be aware of its value. The data described in this study also suggests modifications to the initial research model.

The primary analysis performed was term occurrence, with the goal of producing a pattern or common trend. Correlation analysis is not applicable in this case. Results emanated from the following analysis (Schutt 1999):

- Reviewing research notes to identify important statements and possible ways of coding the data.
- Determining how many people made a particular type of comments?
- Determining if and how often did the social interaction lead to arguments/disagreements?

Interviews, a focus group, artifact analysis and an observation of a disaster recovery test all indicated the same two 'reliance' themes: disaster recovery documentation is not relied upon during a disaster and the recovery of information systems is heavily reliant on humans.

Results

During the analysis of the interviews and focus groups, a number of consistent themes emerged. Undoubtedly, the most common, and passionate statements made during the research involved the immediate desire to check on the safety of family members once the attacks started. These observations signal the importance of recognizing the primacy of relationships people have with their families (Paton 1997). The focus on family has therefore created communication and coordination difficulties with public officials and other organizations in certain situations (Bolin and Borton, 1986).

There was universal agreement across all research participants (the ten focus group participants and six interviews) that during September 11, 2001, disaster recovery plans were not used. The rationale was varied, including availability of the plans, lack of confidence in the plan themselves and the 'ridiculous idea' of reading a plan while buildings are falling. The research has shown that organizations often create elaborate emergency operations plans, but they fail to develop the capability to implement these plans (Auf Der Heide 1989). Disaster plans are important, but they are not enough by themselves to assure preparedness. They can be an illusion of preparedness if they are not tied to training programs, not acceptable to the intended users, not tied to the necessary staff or other resources, or not based on valid assumptions. This illusion is called the 'paper plan syndrome' (Auf der Heide, 1989). The terms 'lack of confidence' and 'incomplete' were the term most commonly used by every interviewee and member of the focus group as a rationale of not using the documented DR plans. Those preparing for disasters should therefore ensure that their plans are realistic and achievable in practice. The most memorable comment was: "With a building falling down, who will locate or print a 300 page document and start reading?" Of course, proper management of the disaster recovery plan will ensure all staff are aware of the plans before a disaster strikes.

This study has demonstrated a strong link between people and the recovery of technology. Disaster recovery plans, at best, can be described as inadequate. Specifically, documentation on September 11 was either ignored or useless. As a result, staff required to restore production application relied heavily on their personal relationships with business contacts, DBAs and management. The most fundamental question of the day could not be answered: are we open for business today? This validated the Kasten (2001) study that informally developed teams are more effective than formal teams. This was evident during the disaster recovery test, where the formal plans and assignments in the DR plans were largely ignored, and information and problem solving was performed in the coffee room. Rather than search for the information needed, technologists utilized their personal networks to solve problems. These personal relationships are critical during a crisis and are very informal in nature. During September 11th, 2001 and the days following, those relationships were used for the following:

- Access to production system to update databases (e.g., forcing a business day to close).
- Many people that died on 9/11 played critical roles in firms. Many held passwords and user names for accounts and resources which were crucial for access to business status updates.
- Junior staff member were given access to rooms and data not normally afforded to them, as their managers needed particular sets of data.
- Procedures for software change control (a critical part of controlling information security) were largely suspended for approximately one week following September 11th.
- The concept of a business day no longer existed and individual departments remained open while other departments in the same firm were closed.

The interviews and focus group provided three recommendations that businesses can immediately implement to improve disaster recovery efforts. Also, there was an informal recommendation (also called the 'wink/wink' idea) related to information security.

One unofficial information security recommendation was agreed upon, but the language was debated, leaving the focus group and interviewees to name this item the 'wink wink' recommendation. Information security is critical in large firms and is often very cumbersome. The reality is that during a crisis, 'brute-force' measures require some policies to be circumvented. All agreed that information policies can't be stopped during a crisis, but they need to be relaxed. Due to the human elements and personal relationships, firms need to realize that information system will be changes in an un-controlled manner during a disaster. How these changes conflict with existing information security and change control policies presents an issue for firms.

Although this study was primarily focused on the events of September 11, 2001, several member of the focus group expressed concern with the growing trend in disaster recovery. The 'worst-case' has occurred and it seems that the planning is now geared for an all-out terrorist attack and ignores the medium sized crisis that happens on a weekly basis. The topic was probably raised due to the fact that the focus group was held on a day when torrential rain forced mass transit in New York City to a virtual stop. Many people could not make it to their offices that day, and remote access capabilities (the ability to work from home) for many firms could not handle the volumes. Another example occurred on February 12th and 13th, 2008. New York City experienced an ice, snow and heavy rain event. As a result, many staff left early to avoid commuting problems. A quick discussion with two members of the focus group indicated that the remote access capabilities could not handle the volume that evening. It calls into question how viable is the plan to have entire divisions work from home during a crisis.

One area of great debate in the focus group was the role of government surveillance in information systems. This is the 'information management versus information legislation' debate. This often heated discussion centered on the concept of expanding government surveillance of information systems. The argument for increased surveillance and government oversight was based on the government's need to be proactive in an ever changing technology world. Terrorists are very familiar with banking and financial rules and have become creative in circumventing the rules to avoid detection. The argument against more legislation, such as the Patriot Act, is that the government already had sufficient information on September 11th that an attack was imminent – the information was simply not managed or communicated properly. It was also interesting to note that the debate did not follow political party affiliations. Make no mistake about this topic; people on both sides of the argument were passionate in their beliefs.

This research demonstrated clear and heavy dependence on human intervention in the recovery of information systems. Many participants used the term 'brute force' to describe the Herculean effort it took to re-establish the Wall Street IT infrastructure and highlighted the lack of confidence information technology staff shows in disaster recovery planning.

The events on September 11, 2001 also demonstrated the fluid nature of management skills during a crisis. In the days and weeks following September 11, 2001, managers were called upon to perform new and unique tasks.

A study of professional emergency managers illustrated the importance of leadership skills and abilities (Drabek 1987). The survey indicates that effective emergency managers are able to motivate

others and harness their knowledge and contributions for disaster preparedness. Capable emergency managers also are able to compromise, mediate and facilitate in difficult situations. Finally, strong emergency managers communicate effectively, are highly organized, and are able to maintain control under stressful situations. Emergency managers will be required to make decisions with incomplete or inaccurate information in a period of changing and possibly hazardous conditions. In addition to the 'disaster itself', this research documented that inaccurate information will be disseminated during a crisis, thus compounding an already difficult situation. Previous studies have discovered that information outside of official channels may be lacking or inaccurate (Britton 1989). Sensationalizing, misreporting, or generating rumors about the response and/or how it was managed are prominent stressors in this situation (Patton 2003).

The research study presented an intimate view of the complex nature of people during a crisis of enormous magnitude. It demonstrated the continued reliance and dependency on humans to resolve disaster incidents. As the events of September 11, 2001 unfolded, their skills and dedication were critical factors in the recovery of Wall Street firms. Many participants in the research made an incorrect assumption regarding the study, believing that the goal of designing a disaster recovery plan should be absolutely no human interaction, and that information systems should be 'self-correcting.' The goal of the research was to define the human aspects of the Wall Street recovery on September 11, 2001, not to eliminate those roles (unrealistic). Quite to the contrary, this research demonstrates clearly that due to the complexity of modern information systems, human intervention will be required for the foreseeable future and needs to be accounted for in the design of information systems.

Resources and references

Agada, J. (1999). Inner-city gatekeepers: an exploratory survey of their information use environment. *Journal of the American Society for Information Science and Technology*, 50(1), 74-85.

Auf der Heide, E. 1989. *Disaster Response: Principles and Preparation and Coordination*, The C.V. Mosby Company, St. Louis, MO.

Beacham, A.E. and McManus, D.J. 2004. "Recovery of financial services firms in the World Trade Center, post September 11, 2001/01". *Information Systems Security*. Volume 13. Number 2. (May-June 2004): Page: 46-55.

Beckett, Paul, and Jathon Sapsford. 2001. "Rebuilding Wall Street: How Wall Street's Nervous System Caused Pain". *Wall Street Journal*, September 21, 2001.

Blanchard, B.W. 1984. *American Civil Defense 1945-1984: The Evolution of Programs and Policies*, National Emergency Training Center, Federal Emergency Management Agency, Emmitsburg, MD.

Blustein, Paul, and Kathleen Day. 2001. *Industrialized Nations Act to Reassure World*. *Washington Post*. September 13, 2001.

Case. 2002. in Johnson, C.A. "Choosing people: The role of social capital in information seeking behaviour". *Information Research*. Volume 10. Issue 10. (2004).

*Note: Available at <http://InformationR.net/ir/10-1/paper201.html>.

Castells, Manuel. 2003. *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford University Press. (April 2003).

Choo, C.W. (1993). *Environmental scanning: acquisition and use of information by chief executive officers in the Canadian telecommunications industry*. Unpublished Ph.D. Thesis, University of Toronto, Toronto.

Connell, Rory. *Collective Behavior in the September 11, 2001 Evacuation of the World Trade Center*. Disaster Research Center. University of Delaware. Newark, DE 19716. Available at:
<http://dspace.udel.edu:8080/dspace/bitstream/19716/683/1/PP313.pdf>.

Conway, Steve, Ian Combe and David Crowther. 2003. Strategizing networks of power and influence: the Internet and the struggle over contested space. *Managerial Auditing Journal*. Volume 18. Number 3. pp. 254-262. Available at:
<http://www.emeraldinsight.com/insight/ViewContentServlet?Filename=Published/EmeraldFullTextArticle/Articles/0510180308.html>

Costa, Thomas F. 2001. *Important Notices*. September 12 and following. New York, NY:Government Securities Clearing Corporation.

Drabek, T.E. 1987. *The Professional Emergency Manager*, Institute for Behavioral Science, Boulder, CO,.

Eisenstein, Elizabeth L. 1979. *The Printing Press as an Agent of Change*. N.p.: Cambridge University Press.

Ferre, Frederick. 1988. *Philosophy of Technology*. Engelwood Cliffs, New Jersey: Prentice Hall.

Fisher, K. E. 2004. "Information behaviour of Migrant Hispanic Farm Workers and Their Families in the Pacific Northwest". *Information Research*. Volume 10. Issue 1.

*Note: Available at <http://InformationR.net/ir/10-1/paper199.html>

Irwin, R.L. 1989. "The Incident Command System (ICS)". *Disaster Responses: Principles of Preparation and Coordination*. Mosby, St Louis, MO.

Johnson, C.A. 2004. "Choosing people: The role of social capital in information seeking behaviour". *Information Research*. Volume 10. Issue 1.

*Note: Available at <http://InformationR.net/ir/10-1/paper201.html>

Johnston, Barry, Oana M. Nedelescu. (2006). [The impact of terrorism on financial markets](#). *Journal of Financial Crime*. Volume: 13. Issue: 1; 2006. Research paper.

Kasten, Joseph. 2001. "Knowledge Strategy Drivers: An Exploratory Study". A Dissertation Submitted to the Faculty of Long Island University by in partial fulfillment of the requirements for the degree of Doctor of Philosophy. November 10, 2001.

Krebsbach, K. 2004. "Banks, the reluctant warriors [disaster recovery for terrorist threats]". *US Banker*. Volume 114. Number 9. (Sept. 2004): Page: 22.

Lacker, Jeffrey M. 2003. "Payment System Disruptions and the Federal Reserve Following September 11, 2001." *Federal Reserve Bank of Richmond, Richmond, Virginia, 23219, USA*. December 23, 2003.

Available at:

http://scholar.google.com/scholar?hl=en&lr=&q=cache:4MXjwHBHq8EJ:www.rich.frb.org/pubs/working_papers/pdfs/wp03-16.pdf+system+outages+9+11+financial+services

Leckie, G.J., Pettigrew, K.E., & Sylvain, C. (1996). Modeling the information seeking of professionals: a general model derived from research on engineers, health care professionals, and lawyers. *Library Quarterly*, 66(2), 161-193.

- McEntire, David A. 2004. "Development, disasters and vulnerability: a discussion of divergent theories and the need for their integration". *Disaster Prevention and Management*. Jul 2004. Volume: 13. Issue: 3. Page: 193 – 198.
- Mackenzie, Donald A., and Judy Wajcman, eds., 1999. *The Social Shaping of Technology*. Open University Press.
- Martin, Henri-Jean. 1994. *The History and Power of Writing*. Chicago: University of Chicago Press.
- Moss, Mitchell L., Anthony M. Townsend. 2006. "Disaster Forensics: Leveraging Crisis Information Systems for Social Science". Available at: <http://urban.blogs.com/research/files/Moss-Townsend-ISCRAM2006-final.pdf>. Last Visit: 01/01/2007.
- Oz, Effy. 2003. *The World Trade Center Disaster: A Study on Business Continuity Planning at Organizations*
- Paton, Douglas. 1997. "Post-event support for disaster workers: integrating recovery resources and the recovery environment". *Disaster Prevention and Management*. 1997. Vol. 6, Issue. 1; pg. 43.
- Quarantelli, E.L. (1984), *Organizational Behavior in Disasters and Implications for Disaster Planning*, Monograph Series, Vol. Vol. 1 No.2, pp.1-31.
- Quaantelli, E.L. 2005. *Catastrophes are Different from Disasters: Some Implications for Crisis Planning and Managing Drawn from Katrina*. Available at: http://www.unitedsikhs.org/katrina/catastrophes_are_different_from_disasters.pdf. Last Visit: 01/02/2007.
- Quaantelli, E.L. (Editor). 1998. *What is a Disaster? Perspectives on the Question*. Routledge. New York, New York. Notes: Article(s) contributed by: Claude Gilbert, Wolf R. Dombrowsky, Gary A. Kreps, Boris N. Porfiriev, Kenneth Hewitt, Russell R. Dynes, Robert A. Stallings, Uriel Rosenthal, Steve Kroll-Smith, Valerie J. Gunter, Anthony Oliver-Smith, Ronald W. Perry, Russell R. Dynes, Anthony Oliver-Smith.
- Schutt, Russell K. 1999. *Investigating the Social World*. Thousand Oaks, California: Pine Forge Press.
- Seifert, J.W. 2002. "The effects of September 11, 2001, terrorist attacks on public and private information infrastructures: a preliminary assessment of lessons learned". *Government Information Quarterly*. Volume 19. Number 3. (2002): Pages: 225-242.
- Sikich, Geary W. 2003. *Integrated Business Continuity: Maintaining Resilience in Uncertain Times*. Tulsa, Oklahoma: Penwell Corporation. 2003.
- Warner, E.S., Murray, A.D., & Palmour, V.E. (1973). *Information needs of urban residents*. Baltimore, MD: Regional Planning Council. (Final Report Contract No. OEC-0-71-4555)
- Webster, Frank. 1995. "Theories of the Information Society". 1995. Routledge. London.
- Winner, Langdon. 1986. *The Whale and the Reactor: A Search for Limits in an Age of High Technology*. N.p.: University of Chicago Press.

Copyright

The Business Continuity Journal is Copyright 2011 Portal Publishing Ltd, all rights reserved.

ISSN

ISSN 1752-4539

Publisher and other contacts

Publisher

Portal Publishing Ltd, PO Box 1393, Huddersfield, HD1 9TN England
Telephone: +44 1484 300750

Editor

David Honour editor@businesscontinuityjournal.com

Subscriptions subs@businesscontinuityjournal.com