Facilitated Process for Improving Organizational Resilience

Sonia McManus[1]; Erica Seville[2]; John Vargo[3]; and David Brunsdon[4]

Abstract: Resilient organizations contribute significantly to resilient communities. However, the task of building more resilient organizations is complicated by an inability to translate the concept of resilience into tangible working constructs for organizations. In addition, resilience is often considered to be a crisis or emergency management issue. The link between creating resilient day-to-day operations and having a resilient crisis response and recovery is typically not well understood by organizations. Resilience for organizations is found to have three principal attributes. Situation awareness, management of keystone vulnerabilities, and adaptive capacity. A facilitated process is introduced that assists organizations to enhance their performance in relation to these attributes. This process is called resilience management and was developed and tested with 10 case study organizations selected specifically to represent a wide range of industry sectors, business types, and sizes in New Zealand. Some of the preliminary resilience issues to arise from this study are also briefly discussed.

DOI: 10.1061/(ASCE)1527-6988(2008)9:2(81)

CE Database subject headings: New Zealand; Resilience; Risk Management; Organizations; Planning.

Introduction

The intrinsic relationship between the resilience of organizations and achieving more resilient communities is not often appreciated, particularly by the organizations themselves. Organizations provide services, cash flow, and employment to communities. The ability of organizations to keep operating in times of adversity is a significant element in the recovery and health of the wider community following a crisis. Furthermore, there is an increasing appreciation of the interconnectedness of modern organizations and the associated vulnerabilities that this introduces. Other issues that contribute to a desire for more resilient organizations is the increasing reliance on technology and technology providers. Consumers and communities are increasingly demanding that organizations exhibit high reliability in the face of adversity and that decision makers are able to address not only the crises that they know will happen, but also those that they cannot foresee. There are several authors who have investigated the nature of these types of organizations and how they address unexpected failures of their operating systems, as well as the increasing occurrence of natural disasters and the escalating vulnerability of communities; the reader is directed to these for a more detailed discussion (Barabasi 2003; Perrow 1984; Watts 2003; Weick and Sutcliffe 2001).

A significant issue in creating resilient organizations is promoting a greater understanding of what resilience means to organizations both from a day-to-day perspective and as a means to an improved crisis response and recovery. Furthermore, it is important that organizations adequately translate the concept of resilience into tangible working constructs that are practical and effective in the short and long term. This paper looks at a definition of resilience for organizations and introduces a facilitated resilience management process to provide practical tools for achieving improved resilience. This research has used information from 10 case study organizations to identify key resilience issues in New Zealand, and preliminary findings are presented in this paper, together with recommendations for future work to enhance these findings.

What Is Organizational Resilience?

In New Zealand, there is an increasing emphasis on creating more resilient communities. The link between the resilience of communities and the resilience of the organizations that serve those communities is partially the focus of a six-year research project in New Zealand (Resilient Organizations 2006). This project seeks to identify the key elements of organizations in the New Zealand context that make them more or less resilient in the face of crisis situations, and use these findings to develop strategies for improving organizational resilience.

Increasingly the focus is moving from looking at tools to assist the crisis response towards tools that contribute to improved preparedness before a crisis hits. The changed focus from postcrisis response to precrisis planning originated in the early-mid 1990's in New Zealand and reflects a global trend (Britton and Clark 2000; Buckle et al. 2000; Keanini 2003; Luers and Lobell 2003; McEntire 2001; Pelling and Uitto 2001; Weichselgartner 2001).

In New Zealand during the 1980s, significant and widespread economic restructuring highlighted the need to alter the way

[1]Resilient Ventures Ltd., 16 Surfers Pl. North Beach, Christchurch 8083, New Zealand. E-mail: sonia@resilientventures.co.nz

[2]Resilient Organisations Research Programme, Dept. of Civil Engineering, Univ. of Canterbury, Private Bag 4800, Christchurch 8140, New Zealand. E-mail: erica.seville@canterbury.ac.nz

[3]Dept. of Accountancy, Finance and Information Systems, Univ. of Canterbury, Private Bag 4800, Christchurch 8140, New Zealand. E-mail: john.vargo@canterbury.ac.nz

[4]Director, Kestrel Group Ltd., P.O. Box 5050, Wellington 6145, New Zealand. E-mail: db@kestrel.co.nz

Note. Discussion open until October 1, 2008. Separate discussions must be submitted for individual papers. To extend the closing date by one month, a written request must be filed with the ASCE Managing Editor. The manuscript for this paper was submitted for review and possible publication on July 28, 2006; approved on March 23, 2007. This paper is part of the ***Natural Hazards Review***, Vol. 9, No. 2, May 1, 2008. ©ASCE, ISSN 1527-6988/2008/2-81–90/$25.00.

Nat. Hazards Rev. 2008.9:81-90.

emergency management was addressed, resulting in legislative changes and the establishment of the Ministry of Emergency Management in 1999 (subsequently renamed Ministry of Civil Defence and Emergency Management). The purpose of these changes was to ensure that broad risk management techniques became embedded in government, business, and the community, thereby increasing overall resilience and continuity (Britton and Clark 2000). The current legislation in New Zealand for Civil Defence and Emergency Management (CDEM Act 2002) reflects a need for greater levels of responsibility from organizations with a front-line response during and following a crisis. However, it is becoming apparent that a wider range of organizations also need to increase their resilience because of the vital roles that they play in longer term community resilience and recovery (Dalziell 2005) and the vulnerability of links between these organizations.

Interdependence between organizations in New Zealand was highlighted by a landmark study looking at the performance of lifeline utility organizations in a large scale hypothetical earthquake scenario in Wellington, the nation's capital (CAE 1991). The interface with coordinating organizations such as Civil Defence was illustrated in this study as a critical facet to the successful response and recovery of lifeline utilities and the wider community that they serve. Furthermore, this study identified that individual organizations must create their own emergency planning strategies and be involved with the strategies of those on whom they will depend in a crisis. The Wellington Lifelines study, and the others in New Zealand that followed this model, clearly showed that interdependence of utilities is made more vulnerable by our increasingly sophisticated world and our reliance on advanced technology. The vulnerability associated with interdependency is further enhanced by expectations of the general public for both private and public organizations to display more accountability in a crisis situation (WELG 1994).

A total of 10 case study organizations were used in this study. It became quickly apparent that there were three main barriers to developing increased resilience in these organizations. The first, was a limited awareness of the organization's entire operating environment. This included the wider community of stakeholders and their expectations and limitations, as well as poor understanding of the range of hazard types and their consequences that were likely to be important. Second, there was a need to better identify and manage the principal or keystone vulnerabilities and ensure that each organization could prioritize available resources to best advantage. Finally, the culture of the organizations and their ability to remain flexible and adaptable was a critical feature of their overall resilience. These three key areas were identified in the broader sense of organizations as complex adaptive systems in an increasingly global network. From these observations and a review of the literature, a definition of resilience was introduced: *Resilience is a function of an organization's overall situation awareness, management of keystone vulnerabilities, and adaptive capacity in a complex, dynamic, and interconnected environment*.

Traditionally, resilience is viewed as the qualities that enable the individual, community, or organization to cope with, adapt to, and recover from a disaster event (Buckle et al. 2000; Horne 1997; Mallak 1998; Pelling and Uitto 2001; Riolli and Savicki 2003). Although the term resilience has its roots in science as the ability of materials to return to their original form following deformation (Sheffi 2006a), it is also used to describe the capacity of a system to absorb change (generally conceptualized in the form of sudden shocks) and still retain its essential functionality (Walker et al. 2006). Evolution of the original concept of resilience has occurred through its application in numerous scientific disciplines. Resilience has been discussed in relation to climate change and linked to vulnerability (Timmerman 1981), in terms of proactive and reactive resilience of society as a whole (Dovers and Handmer 1992), as it relates to both ecological and social systems (Adger 2000), and natural hazards (Blaikie et al. 1994), to name but a few. Several excellent reviews of the literature are presented by Klein et al. (2003), Folke (2006), and Hollnagel et al. (2006) and the reader is directed towards these for a detailed discussion. However, as pointed out by Klein et al. (2003), resilience remains a theoretical concept and methods for achieving improved resilience at an operational level still challenge both the academic and the practitioner. The following discussion offers a more detailed analysis of each of these three attributes of organizational resilience: Situation awareness, management of keystone vulnerabilities, and adaptive capacity.

Situation Awareness

It is critical that organizations understand that they do not work alone if they are to successfully navigate a crisis. They must recognize themselves as parts of a wider network, and indeed as networks themselves. As a result, there is an increasing need for decision makers, and organizations generally, to have common and shared situation awareness. Originally coined in relation to military pilots, the modern concept of situation awareness is traditionally attributed to Endsley (1995) and described the situation awareness of an individual within a system. However, as recognition of teamwork increased, so did the necessity to look at situation awareness from a different, more complex perspective. While team or shared situation awareness is rapidly becoming a significant field of research, there is no agreed upon definition Salmon et al. (2006) and the terminology is diverse [see Roth et al. 2006; Rognin (2000); Cannon-Bowers et al. (1993); Espinosa et al. (2004); and Gutwin and Greenberg (2004) for examples]. Oomes (2004) suggests the concept of organizational awareness, particularly in relation to the effective management of crisis situations, where organizational awareness is: "*… an understanding of the multiple parties that make up the organization and how they relate to each other*."

Events such as the 9/11 terrorist attacks in the United States, Hurricane Katrina in 2005, and the Boxing Day Tsunami in 2004 have highlighted how poor communications, limited situation awareness, and a lack of multiagency/organization interoperability has contributed to major deficiencies in the emergency response (Bahora et al. 2003; Titan Systems Corporation 2002; Ntuen 2006; Runyan 2006). Researchers and practitioners are, therefore, becoming increasingly concerned with developing improved situation awareness among teams. Essentially, situation awareness is "the engine that drives the decision making and performance in complex, dynamic systems" (Endsley et al. 2003).

A fundamental approach to increasing an organization's situation awareness is by encouraging some experience of pseudocrisis situations through the use of scenario exercises. Coates (2006) suggests that organizations have a "severely limited psychological capacity" to look at incidents in other corporations and apply the lessons learned to themselves. Therefore, scenario exercises offer significant value for the networked organization, specifically if they involve participants from across a number of internal divisions and/or external interconnected organizations.

Improving an organization's situation awareness about crises also involves learning about the types of emergency situations that may occur. Many organizations have engaged in some sort of risk identification process, but few take this process one step fur-

Nat. Hazards Rev. 2008.9:81-90.

ther and combine risks of similar nature or expected response. In an emergency, often the same types of issues will be faced and actions will be common across crisis types (Pearson and Mitroff 1993).

Therefore, in this study, situation awareness is defined as a measure of an organization's understanding and perception of its entire operating environment. This includes the ability to look forward to opportunities as well as potential crises and the ability to identify crises and their consequences accurately. Further, situation awareness includes an enhanced understanding of the trigger factors for crises, an increased awareness of the resources available both internally and externally, and a better understanding of minimum operating requirements. Critically, situation awareness also incorporates an enhanced awareness of expectations, obligations, and limitations in relation to the community of stakeholders, both internally (staff) and externally (customers, suppliers, consultants, etc.).

Management of Keystone Vulnerability

The term vulnerability is one that has many different definitions and applications, depending on the objectives of the researchers/practitioners and the situation within which it is applied. As such, there is considerable confusion over the use of the term vulnerability and assessing and modeling vulnerability in the real world. The concept of vulnerability originated in natural hazard research, but has since expanded considerably into other disciplines. There are many authors who have sought to summarize the thinking about vulnerability; however, this is an extremely difficult task as the literature on the topic is large. For this research, vulnerability is considered specifically as it relates to organizations and makes no attempt to provide a detailed account of vulnerability in other areas of enquiry. Good summaries are given by Klein et al. (2003), Villagrán De León (2006), and Füssel (2005).

A number of studies of organizational vulnerability have highlighted some of the strongest influences on postcrisis survival, particularly for small businesses. The degree of structural damage to the physical location of an organization and its degree of disaster preparedness has been shown to have some influence on business survival rates (Alesch and Holly 1998; Alesch et al. 2001; Chang and Falit-Baiamonte 2002; Tierney 1997; Webb et al. 2003). However, much stronger indicators of organizational failure following a crisis include interruptions to infrastructure, experiencing financial difficulties prior to an event, operational difficulties, problems with interdependencies, and problems with the supply chain (Durkin 1984; Alesch and Holly 1998; Alesch et al. 2001; Tierney 1997; Webb et al. 2003; Chang 2001a,b; Chang and Falit-Baiamonte 2002).

The scale at which vulnerability is assessed is critical and the global and interconnected nature of organizations highlights this fact. For example, Adger et al. (2004) state that vulnerability should not be assessed across scales because processes causing the vulnerability are different at each scale. Important also to any vulnerability research is awareness of the spatial-temporal element (Watts and Bolhe 1993), suggesting that vulnerability is not a static entity, but is contextual. From this perspective, a more holistic and systemic approach to vulnerability may be more suitable for organizations. Villagrán De León (2006) introduces the notion that a community or society be viewed as a set of interconnecting systems and networks. The individual components of these systems must be assessed for their vulnerability together with the vulnerability of the relationships and interactions between these components. Therefore, the intrinsic connectivity of organizations, together with the interdependencies that arise as a result, have a significant impact on organizational vulnerability.

This study uses the term "keystone" when considering vulnerabilities. Keystone can be used to denote the presence of integral species in an ecosystem; one that has an influence on its environment or ecosystem that is disproportionate to its size or abundance and the loss of this species can cause a significant shift in the ecosystem, sometimes causing its eventual destruction. Keystone can also have an architectural meaning, representing "the wedge-shaped piece at the highest point of an arch that locks the other pieces in place" or "something on which associated things depend for support" (New Penguin English Dictionary 2000). These keystone vulnerabilities are components in the organizational system, which by their loss or impairment, have the potential to cause exceptional effects throughout the system; associated components of the system depend on them for support. Keystone vulnerabilities may be either catastrophic (the immediate failure of a system due to the sudden loss of a critical component) or insidious (the failure of a system over time due to ongoing systematic or coincident loss of moderately critical components).

The definition in this study of the management of keystone vulnerabilities relates to those aspects of an organization, operational and managerial, that have the potential to have significant negative impacts in a crisis situation. There are two aspects to identifying keystone vulnerabilities. The first is the speed at which a component failure has a negative impact (rapid or insidious), and the second is the number of component failures required to have a significant negative impact on an organization (discrete or cascading). Keystone vulnerabilities may include specific tangible organizational components such as buildings, structures, and critical supplies, or computers, services, and specialized equipment. Tangible components can also include, for example, individual managers, decision makers, and subject matter experts. Keystone vulnerabilities can also include less tangible components, for example, relationships between key groups internally and externally, communications structures, and the perception of the organizational strategic vision.

Adaptive Capacity

The literature in relation to adaptive capacity is divided into two rather distinct categories. There is a huge body of research on adaptive capacity as it relates to socioenvironmental systems, particularly in relation to climate change research. This work is matched by the volumes of research into organizational adaptive capacity. This discussion focuses on the organizational research domain. For excellent summaries of adaptive capacity in socioeconomic systems, the reader is referred to Klein et al. (2003), Brooks (2003), Gallopin (2006), and Smit and Wandel (2006).

For the purposes of this study, adaptive capacity is a measure of the culture and dynamics of an organization that allow it to make decisions in a timely and appropriate manner, both in day-to-day business and also in crises. Adaptive capacity considers aspects of an organization that may include (but not be limited to) the leadership and decision making structures, the acquisition, dissemination and retention of information and knowledge, as well as the degree of creativity and flexibility that the organization promotes or tolerates.

The concept of adaptive capacity is at the core of current organizational resilience methodology. Adaptive capacity is defined as the ability of an enterprise to alter its "*strategy, operations, management systems, governance structure, and decision-support capabilities*" to withstand perturbations and disruptions (Starr

Nat. Hazards Rev. 2008.9:81-90.

et al. 2004). Organizations that focus on their resilience in the face of disruption generally adopt adaptive qualities and proactive responses. Furthermore, they emphasize positive behavior within the enterprise and within employees, and look at disruptions as being opportunities for advancement (Mallak 1998; Folke et al. 2002).

The study of adaptive capacity in relation to organizational systems has resulted in considerable advances in recent years, particularly regarding the cultural capital of an organization and the effects this may have on its ability to withstand crises. Many organizations have been shown to exhibit favorable workplace cultures that help them to adapt to changes in their operating environment, even when these changes are unforeseen and unexpected. Examples include Nokia, Toyota (Sheffi 2006a), Dell (Sheffi 2005), UPS (Coutu 2002), and Coca-Cola (Seaman and Williams 2005). While terminology differs regarding what attributes actually make up such effective organizational cultures, there are some widely accepted qualities that organizations can encourage. For example, the ability of both leaders and general staff to view crises from a positive and opportunistic perspective is important in the adaptive organization (Borneman 2005; Hagevik 1998; Norman et al. 2005; Pearson and Mitroff 1993; Penrose 2000; Sheffi 2005; Starr et al. 2004). The quality of leadership and the degree of empowerment through to lower levels in an organization is increasingly seen as a critical facet of an adaptive organization's culture (Sheffi 2006a, b, 2005; Kerfoot 2005; Hagevik 1998; Norman et al. 2005; Coutu 2002). Empowerment, for instance, has been identified as a key part of the successful response by the U.S. Coast Guard during Hurricane Katrina and the saving of over 24,000 lives (Sheffi 2006b).

The interest in creating an increased adaptive capacity during and immediately following a disaster has led some researchers to propose a set of adaptive features to enhance organizational and societal resilience (Weick 1993; Kendra and Wachtendorf 2003; Mallak 1998). This includes, for example, bricolage, which is the capacity to adapt known information and apply it to the current situation in a creative manner, and virtual role systems, the ability of subsets of an organization to take on the role and responsibility of absent members.

Other features include wisdom or the capacity to know the limits of the information at hand, and the ability to seek out additional information, respectful interaction, positive adaptive behavior, and the development of a tolerance for uncertainty (Weick 1993).

Dalziell and McManus (2004) introduce the concept that systems (specifically organizational systems) can adapt to changes in different ways. First, they may use existing responses and apply them to the problems at hand, which may involve upscaling this response. Second, existing responses may be utilized in a new context for a crisis situation. Third, an organization may develop novel responses and apply them to a problem. The problems may be new and unforeseen or those that the organization has been able to see coming. Typically, organizations enlist either a command and control type structure to deal with crisis or a more organic and innovative approach (Dalziell and McManus 2004). Recent research is pointing to the increased ability of organizations to respond effectively using a more creative and flexible decision making structure. This appears to be because automation and rigor (more associated with command and control decision making) may actually hinder adaptive capacity by reducing situation awareness (Endsley et al. 2003) and ultimately performance; systems must be more flexible or they risk becoming redundant (Stanton and Baber 2006).

In addition to offering organizations a specific definition of resilience, this study focused on the development of a suite of tools that could provide organizations with practical means to first assess and then improve their overall resilience. This process is called resilience management and allows organizations a platform from which they can begin to put theoretical concepts and definitions of resilience into practice. The elements of resilience management are discussed below.

Process for Improving Organizational Resilience

An organization with a heightened resilience is one that is more likely to weather both the problems of day-to-day business and successfully navigate the issues that arise in a crisis and has three main qualities above a nonresilient organization. First, a resilient organization has a greater awareness of itself, its key stakeholders, and the environment within which it operates, both on a day-to-day basis and in emergency situations. Second, it has an increased ability to identify and manage its keystone vulnerabilities including the positive and negative impacts that these could have for the organization in a crisis. Third, a resilient organization has the ability to adapt to changed situations with new and innovative solutions and/or the ability to adapt the tools that it already has to cope with new and unforeseen situations.

As previously discussed, it is important that resilience becomes more than a theoretical concept and offers organizations with practical tools and tangible outcomes. While planning for risk management, business continuity and emergency management is often seen as intrinsically linked; a practical means of linking this planning is often absent. Therefore, the authors propose the use of a resilience management process; an approach that utilizes existing planning strategies in an organization and provides an overarching and holistic platform from which to manage them. Implementation of the resilience management process will help an organization to successfully navigate the crisis response and recovery period by integrating resilience into day-to-day business. This integration is achieved by encouraging increased situation awareness, improved adaptive capacity, and better identification and management of keystone vulnerabilities.

The resilience management process consists of a suite of elements including: Building awareness, selection of essential organizational components, self-assessment of vulnerability, identification and prioritization of keystone vulnerabilities, and increasing adaptive capacity. Each element and the tools available for each element are described below. The elements in this process have been developed and tested with a number of case study organizations as part of this study. These organizations represent different industries, organizational types, and sizes in the New Zealand context.

Building Awareness

In order for resilience management to be effective, an organization must develop a clear understanding and awareness of the issues that contribute to its resilience. This includes the current and projected reality of the organizational operating environment, the resources at the organization's disposal, the expectations and limitations of all stakeholders, and the positive and negative impacts of various types of crises. Awareness is achieved through the use of interviews with key stakeholders, surveys, discussion reports, and by the introduction of consequence scenarios to assist in increasing awareness of hazards and impacts. Interviews and

Nat. Hazards Rev. 2008.9:81-90.

Table 1. Overview of the Consequence Scenarios

Scenario type	Scenario characteristics
Regional event	This scenario tests an organization's response to and recovery from significant physical damage to buildings, contents, and resources, coupled with severe disruptions to lifeline services such as transportation, electricity, water, and telecommunications.
Societal event	This scenario focuses on a nationwide event resulting in extended staffing absences. In this event, all physical infrastructure is intact, but staff are either unable or unwilling to be at work.
Localized event	Scenarios of this nature focus on an organization specific incident resulting in severe disruption to normal operations and reputation impacts and may include loss of life or injury. The intense focus of media and regulatory agencies requires the organization to focus on managing stakeholder perception as well as the physical response and recovery from the event.
Indirect/distal event	This scenario tests organizational response and recovery regarding impacts on business flow through key suppliers or customers. This consequence scenario is designed to explore the ways an organization may be impacted through its networks of interorganizational relationships.

surveying are used to develop a broad understanding of the key issues facing the organization, the extent to which perceptions influence decision making, and the overall degree of awareness in the organization. Discussion reports are an effective way of presenting these findings back to the organization and encourage it to look at itself and its perceptions from an objective external perspective.

A simple technique developed for helping to evaluate an organization's situation awareness is the use of consequence scenarios. These consequence scenarios are used to assess how well an organization understands the types of hazards it may one day face, and the potential impacts these may have on the organization. A set of four consequence scenarios has been developed to help organizations improve their awareness of crises and consequences and are designed to simulate a wide range of potential effects on organizations. Due to the variability in how specific threats may affect an organization, the focus moves from individual hazards to a set of particular event consequences. The scenarios include a regional event that focuses on physical disruption, a nationwide event that concentrates on widespread societal disturbance, a localized event with a focus on reputation impacts, and a distal event that impacts on the business flow and interorganizational relationships. The details of the consequence scenarios are presented in Table 1. The aim of the consequence scenarios is threefold. In the first instance, they encourage organizations to identify events that are foreseeable and consider how they might cope with those outcomes that are not foreseeable. Second, they offer a vehicle for how an organization might address the failure, temporary or otherwise, of linked organizations in both a positive and negative sense. Finally, they allow organizations to prepare for different hazard events that have similar consequences at the same time.

Selection of Essential Organizational Components

Important also is an organization that has an advanced understanding of its essential operational, strategic, and managerial components from both an internal and external perspective. The selection of organizational components is a critical step in the success of the resilience management process because it requires a good understanding of the organization and its intrinsic interdependencies. Some components will differ between organizations and will depend largely on the scale of the investigation and detail of study required, although there are some components that are common to most organizations. Table 2 illustrates the types of generic components identified in this study.

There is a distinction between internal components and external components for an organization. Internal components are those that the organization has the direct ability to manage in terms of resilience. For example, employment contracts with staff

Table 2. Generic Organizational Components

Physical components		Human components		Process components	
(a) Internal components					
Buildings and equipment	Offices	Communication and relationships	General staff	Direct planning	Risk management
	IT hardware		Senior staff		Continuity planning
	Security		Board		Emergency management
	Vehicles	Management	Leadership		Cash flow
	Software/IP		Succession		Market/brand knowledge
	Inventory		Staff welfare		Insurance/aid
Services	Generators	Information/knowledge	Backup		
	Fuel Supplies		Privacy/protection		
	IT networks		Training/review		
(b) External Components					
Services	Electricity	Communication and relationships	Emergency services	Indirect planning	Interconnectedness
	Water		Local authorities		Statutory compliance
	Sewerage		Customers		Contracts
	Telecommunications		Suppliers		Reputation/image
	Transportation		Media		

Nat. Hazards Rev. 2008.9:81-90.

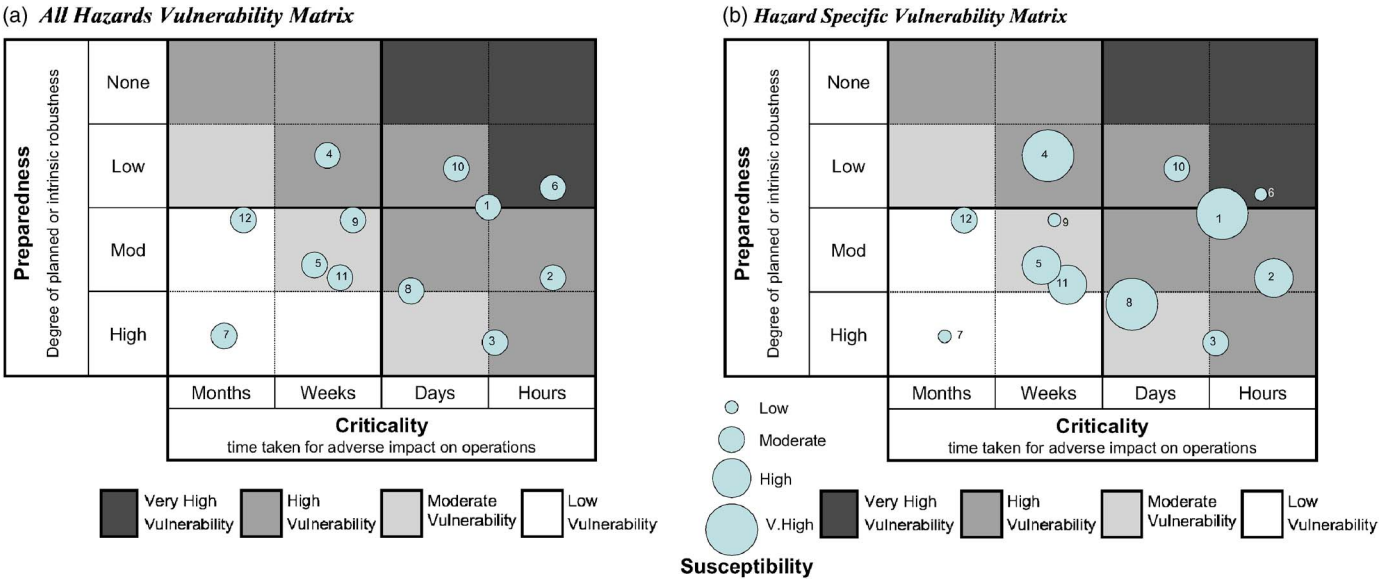

Fig. 1. Sample vulnerability matrices showing (a) an all-hazards approach; (b) a context specific approach to determine keystone vulnerabilities for organizational resilience. Matrix A shows organizational components from an all-hazards context. Circles represent individual organizational components. Matrix B shows organizational components in a context specific matrix. Circle size represents susceptibility to a given context.

would be an internal component. External components, on the other hand, are those that, while potentially having some influence over component management, an organization had no direct ability to change. For example, the supply of telecommunications services by a third party supplier would be an external component, because although the organization may be able to manage its response to such an outage, it cannot control the cause of that outage. Selection of the organizational components is a process that can be repeated at varying scales, and the organization can look at its structure in increasing detail.

Self-Assessment of Vulnerability

An assessment of vulnerability is important in resilience management because it contributes to increased situation awareness, promotes the development of adaptive capacity, and also gives the organization something tangible to work towards. Vulnerability is self-assessed to improve the organizational buy in and encourage the organization to take ownership of the resilience issues that emerge. As a consequence, the organization is more likely to accept accountability for improving vulnerabilities.

The organizational components that have been selected previously are assessed by the organization according to their criticality for continued operations and the degree of preparedness the organization believes it has in the event of component failure. Assessments are performed initially from an all-hazards perspective for both the response phase and recovery phase of a crisis. Both criticality and preparedness are measured on a qualitative scale ranging from very high, high, moderate, and low for criticality and high, moderate, limited, or none for preparedness. Additionally, an assessment for susceptibility may be performed to determine the variation in influence of components relative to specific events or types of event. Susceptibility considers the negative impact on components from a variety of crisis events and is measured qualitatively: Very high, high, moderate or low negative impact.

Identification and Prioritization of Keystone Vulnerabilities

There are two ways to interpret the vulnerability assessment data. First, this information can be considered from an all-hazards approach using the criticality and preparedness information for both response and recovery phases of a crisis. Second, the susceptibility information can be used to look at particular vulnerabilities for an event type of immediate concern; for example, influenza pandemic or as a review of a previous event.

An organization can use the vulnerability matrix to help identify its keystone vulnerabilities. The vulnerability matrix is similar in structure to traditional risk matrices; for example AS/NZS: 4360 (Joint Technical Committee 2004). The vulnerability matrix is subdivided into different zones representing increasing vulnerability (see Fig. 1); extreme, high, moderate, and low. The components that plot within the extreme or high vulnerability zones on the matrix are those that have the greatest potential to cause most disruption to the organization in times of crisis. As a result, these components require the most immediate attention by the organization in order to increase organizational resilience.

Vulnerability matrices can be produced for an assessment of vulnerability at an all-hazards level using preparedness and criticality data. Additionally, susceptibility information can be used to produce a context specific matrix. Examples of both types of vulnerability matrices are presented in Fig. 1. Criticality is plotted on the x axis and preparedness on the y axis. Each organizational component is represented by a "hole" in the matrix. For the "all-hazards" matrix, all the holes are of equal size and it is their position on the matrix that determines their status as keystone vulnerabilities. Susceptibility data, however, is indicated by different sized "holes;" the larger the "hole," the greater the degree of susceptibility. For these context specific matrices, keystone vulnerabilities are identified both by the size of the hole they produce as well as their position on the matrix.

It is important that the vulnerability matrix be considered as

Nat. Hazards Rev. 2008.9:81-90.

part of an iterative process in achieving improved organizational resilience and not a one-off assessment. The dynamic nature of organizations and the environments within which they operate require that ongoing assessment be conducted to check new structures, strategies, employees, knowledge, and other critical organizational components as and when they occur.

Increasing Adaptive Capacity

Ultimately, resilience management is about providing simple and practical tools for decision makers to assess and increase an organization's resilience for times of crisis. As such, one of the most important tools used in the process is the readiness exercises and disaster simulation (REDS). REDS encourages organizations to experience their vulnerabilities and strengths in a simulated crisis environment and offer a platform from which to critically assess decision making and communications. Scenario exercises help an organization to increase its awareness of the operating environment in a crisis and the potential impacts of different event types. For those organizations that have engaged in producing emergency plans or business continuity planning, scenarios offer an excellent opportunity to test these plans before they are needed in a real situation.

The REDS uses events tailored specifically to each organization. REDS can also be used to simulate either the response period or the recovery period following an emergency because time frames can be incorporated into the REDS. For example, REDS may focus on 4 days after the occurrence of a major regional earthquake, 5 weeks following the outbreak of an influenza pandemic, or 6 months after a major attack on an organization's reputation. REDS can be as detailed or as simple as the organization requires. As a minimum, REDS should be conducted with senior management in an organization, as well as those who would be expected to take on decision making roles during a crisis.

There are six distinct stages, conducted sequentially, of the REDS. Stage 1 involves the subdivision of the group according to the number of participants; ideally there should be no more than 12 participants in groups of six each. Additionally, the selected scenario is presented to the participants. Stage 2 focuses on the group discussion for the response phase of the simulation. Each group is expected to address the following four questions. These involve: Consideration of the major issues to face the organization at the time of the crisis, the main priorities for the organization to consider immediately, identification of lesser priorities and time frames until these are likely to become critical, and finally discussion of what the organization could do prior to the crisis to better prepare for this situation.

Stage 3 offers an external perspective where one participant is taken from each group and asked to consider the scenario from the viewpoint of a key external stakeholder. In Stage 4, participants are encouraged to take a break and facilitators offer comments on how the groups are doing and suggest tips and advice for improvement. The groups then reconvene in Stage 5 to reanswer the same questions from Stage 2 for the recovery phase of the REDS scenario. Finally, Stage 6 concludes the REDS with a group debriefing. This is an important way for decision makers in the organization to create an action plan that can be addressed immediately.

Case-Study Analysis

The resilience management process described in this paper has been developed and tested with 10 case study organizations. These organizations were selected to represent a wide range of industries, organizational sizes and types, both public and private, in New Zealand. The purpose in selecting such a diverse range of organizations was to identify common resilience issues for New Zealand organizations irrespective of these types of characteristics. The first case study organization was the test case and the process in its entirety has since been tested with seven other organizations. Two of the case study organizations have not participated in all five steps at the time of writing. The organizations that have participated in the full resilience management process include, for example, a local government organization, a private manufacturer and exporter, a private contractor, a public infrastructure provider, an education provider, and a wholesale distributor. These organizations range in size from eight employees to greater than 5,000 employees. Some of the organizations are widely dispersed geographically, while some have a much more localized operation and a selection rely, to some extent, on funding from the central government, while the rest answer to a board of directors and private shareholders.

Preliminary results from the case study organizations indicate that some of the key resilience indicators include awareness issues for roles and responsibilities of key stakeholders, as well as for the occurrence and consequences of hazard events. Additionally, the awareness of organizational recovery priorities are likely to contribute to overall resilience. The degree of planning, the links between different planning techniques (risk management, business continuity, and crisis management), and the extent to which an organization engages in crisis exercises, influences the identification and prioritization of keystone vulnerabilities. In terms of adaptive capacity, organizations that display strongly negative impacts of silo mentality, poorly managed communications and relationships with stakeholders, and lack flexible and creative decision making processes are also more likely to experience lowered resilience.

Feedback from the case study organizations on the value of resilience management has been positive. Discussions with key decision makers in the eight case study organizations that participated in the full process indicates that these organizations adopted several of the recommendations that arose from the process, and three of these eight organizations have engaged in resilience management in addition to the study.

There are several recommendations for the future development of resilience management techniques for organizations. First, a more rigid and quantitative framework for assessing resilience is required and will ultimately allow organizations to compare their overall resilience with other organizations. The development of such a framework would also assist in improving the level of engagement with organizations. It is foreseeable that organizations could use their resilience to increase their market value to customers in ways that current risk management techniques do. Further, a maturity model and scale of organizational resilience is required. For organizations to compare themselves to other organizations in terms of resilience, it is vital to clearly determine what a truly resilient organization looks like.

Conclusions

This paper provides researchers and practitioners with a specific definition for organizational resilience and offers a facilitated approach to assessing and improving overall resilience called resilience management. In addition, this paper introduces a suite of

Nat. Hazards Rev. 2008.9:81-90.

tools that can be used to address resilience issues in organizations; tools that have been developed in conjunction with 10 individual organizations in New Zealand.

Resilience for organizations is defined as a function of the overall situation awareness, management of keystone vulnerabilities, and adaptive capacity of an organization in a complex, dynamic, and interdependent environment. Further, situation awareness is defined as a measure of an organization's understanding of its entire operating environment while keystone vulnerabilities are those components of an organization that have the potential to have significant negative impacts in a crisis. Adaptive capacity is defined as the culture of an organization allowing it to make decisions in a timely and appropriate manner, both for business-as-usual and for crisis situations.

The resilience management process has been designed to assist organizations both assess and improve their overall resilience. Critically, the link between developing resilience on a day-to-day basis to achieve enhanced operations and functions, and the ability to successfully cope with crisis situations is the focus of resilience management. The elements of resilience management include building an awareness of resilience issues, the selection of organizational components, a self-assessment of vulnerability, the identification and prioritization of keystone vulnerabilities, and the enhancement of adaptive capacity.

Preliminary findings from using the resilience management process with 10 case study organizations in New Zealand indicate that some of the key indicators of resilience include awareness of stakeholder roles and responsibilities, hazard events and their consequences, together with recovery priorities. The use of specific planning, such as risk management and business continuity planning, together with the ability to link these plans and test them using exercises, are also significant indicators of resilience. Further, silo mentality, poor communications and relationships with stakeholders, and inflexible and uncreative decision making are also likely to have considerable impacts on overall organizational resilience.

Additional work in developing resilience management is helping to identify the most appropriate levels of analysis to enable the greatest improvements in overall resilience in organizations. To date, resilience management has been used with individual organizations predominantly at strategic levels rather than at operational levels throughout an organization. However, a significant advantage of resilience management is its scalability, and the elements of the process can potentially be applied at a variety of organizational levels. Further work is proposed to assess the suitability of the resilience management approach with groups of organizations that have a common purpose or operate within discrete industries; for example, manufacturing organizations or emergency responders.

Acknowledgments

This research is funded by the New Zealand Foundation for Research, Science, and Technology and the University of Canterbury, New Zealand. The writers would also like to thank the organizations that have participated in this study for their enthusiasm, their openness, and their support for the recommendations reached.

References

Adger, W. N. (2000). "Social and ecological resilience: Are they related?" *Progress in Human Geography*, 24, 347–364.

Adger, W. N., Brooks, N., Kelly, M., Bentham, G., Agnew, M., and Erikson, S. (2004). "New indicators of vulnerability and adaptive capacity." *Tyndall Centre for Climate Change Research Technical Rep. No. 7*, Univ. of East Anglia, Norwich, U.K.

Alesch, D. J., and Holly, J. N. (1998). "Small business failure, survival and recovery, Lessons from the January 1994 Northridge earthquake." *Proc., NEHRP Conf. and Workshop on Research on the Northridge, California Earthquake of January, 17, 1994*.

Alesch, D. J., Holly, J. N., Mittler, E., and Nagy, R. (2001). *Organizations at risk, What happens when small businesses and not-for-profits encounter natural disasters?* Public Entity Risk Institute, Fairfax, Va..

Bahora, A. S. et al. (2003). "Integrated peer-to-peer applications for advanced emergency response systems. Part 1, Concept of operations." *Proc., Systems and Information Engineering Design Symp.*, IEEE, Charlottesville, Va, 255–260.

Barabasi, A. (2003). *Linked*, Penguin Group, London.

Blaikie, P., Cannon, T., Davis, I., and Wisner, B. (1994). *At risk, Natural hazards, people's vulnerability, and disasters*, Rutledge, New York.

Borneman, J. (2005). "Recognizing the power of resilience." *Textile World*, 155(6), 28–30.

Britton, N. R., and Clark, G. J. (2000). "From response to resilience: Emergency management reform in New Zealand." *Nat. Hazards Rev.*, 1(3), 145–150.

Brooks, N. (2003). "Vulnerability, risk and adaptation: A conceptual Framework." *Tyndall Centre for Climate Change Research Working Paper No. 38*, Univ. of East Anglia, Norwich, U.K.

Buckle, P., Mars, G., and Smale, S. (2000). "New approaches to assessing vulnerability and resilience." *Australian J. Emergency Management*, 15(2), 8–15.

Cannon-Bowers, J. A., Salas, E., and Converse, S. (1993). "Shared mental models in expert team decision making." *Individual and group decision making: Current issues*, N. J. Castellan, Jr., ed., Lawrence Erlbaum, Hillsdale, N. J.

Centre for Advance Engineering (CAE). (1991). "Lifelines in earthquakes: Wellington case study." *Project Rep.*, Christchurch, New Zealand.

Chang, S. (2001a). "Natural disasters and urban economic change." *Proc., 2001 Meeting of the Association of American Geographers*, New York.

Chang, S. (2001b). "Structural change in urban economies: Recovery and long-term impacts in the 1995 Kobe earthquake." *The Kokumin Keizai Zasshi* (J. Economics and Business Administration), 183(1), 47–66.

Chang, S., and Falit-Baiamonte, A. (2002). "Disaster vulnerability of businesses in the 2001 Nisqually earthquake." *Environ. Haz.*, 4, 59–71.

Civil Defence Emergency Management (CDEM) Act (2002). New Zealand.

Coates, J. (2006). "Anticipating disaster from research, or putting the fear of God into top management." *Res. Technol. Manag.*, 49(1), 6–9.

Coutu, D. L. (2002). "How resilience works." *Harvard Bus. Rev.*, 80(3), 46–55.

Dalziell, E. P. (2005). "Understanding the vulnerability of organizations." *Proc., 1855 Wairarapa Earthquake Symp.*, Te Papa, Wellington, 130–135.

Dalziell, E. P., and McManus, S. T. (2004). "Resilience, vulnerability and adaptive capacity: Implications for systems performance." *Proc., Int. Forum for Engineering Decision Making (IFED)*, Switzerland, ⟨www.ifed.ethz.ch/events/Forum04/Erica paper.pdf⟩.

Dovers, S., and Handmer, J. (1992). "Uncertainty, sustainability and change." *Global Environ. Change*, 2, 262–276.

Durkin, M. E. (1984). "The economic recovery of small businesses after earthquakes; the Coalinga experience." *Proc., Int. Conf. on Natural Hazards Mitigation Research and Practice*, New Delhi, India.

Endsley, M. R. (1995). "Towards a theory of situation awareness in dy-

namic systems." *Hum. Factors*, 37, 32–64.

Endsley, M. R., Bolté, B., and Jones, D. G. (2003). *Designing for situation awareness: An approach to user-centered design*, Taylor and Francis, London.

Espinosa, J. A., Lerch, F. J., and Kraut, R. E. (2004). "Explicit versus implicit coordination mechanisms and task dependencies: One size does not fit all." *Team cognition*, E. Salas, and S. M. Fiore, eds., American Psychological Association, Washington, DC., 107–129.

Folke, C. (2006). "Resilience: The emergence of a perspective for social-ecological systems analyses." *Global Environ. Change*, 16(3), 253–267.

Folke, C., et al. (2002). "Resilience and sustainable development: Building adaptive capacity in a world of transformations." Environmental Advisory Council to the Swedish Government, Stockholm, Sweden.

Fussel, H. (2005). "Vulnerability in climate change research: A comprehensive conceptual framework." *eScholarship Repository*, Univ. of California ⟨http://repositories.cdlib.org/ucias/breslauer/6⟩ (accessed January 3, 2007).

Gallopin, G. C. (2006). "Linkages between vulnerability, resilience and adaptive capacity." *Global Environ. Change*, 16(3), 293–303.

Gutwin, C., and Greenberg, S. (2004). "The importance of awareness in team cognition in distributed collaboration." *Team cognition*, E. Salas, and S. M. Fiore, eds. American Psychological Association, Washington, D. C., 177–201.

Hagevik, S. (1998). "Resilience required (adaptability as a desirable factor in a changing environment)." *J. Environ. Health*, 60(10), 37–39.

Hollnagel, E., Woods, D. D., and Leveson, N., eds. (2006). *Resilience engineering, Concepts and precepts*, Ashgate Publishing Ltd, Aldershot, England.

Horne, J. F. I. (1997). "A new direction: The coming age of organizational resilience." *Business Forum*, 22(2/3), 24–28.

Joint Technical Committee (2004). "Risk management." *AS/NZS No. 4360*: 2004, Joint Australian/New Zealand Standard prepared by the Joint Technical Committee, Standards Association of Australia, Sydney and Wellington.

Keanini, T. (2003). "Vulnerability management technology: A powerful alternative to attack management for networks." *Computer Technology Review*, 23(5), 18–19.

Kendra, J. M., and Wachtendorf, T. (2003). "Elements of resilience after the world trade center disaster: Reconstituting New York City's emergency operations center." *Disasters*, 27(1), 37–53.

Kerfoot, K. (2005). "Building confident organizations by filling buckets, building infrastructures, and shining the flashlight (on leadership)." *Dermatol. Nurs.*, 17(2), 154–157.

Klein, R. J. T., Nicholls, R. J., and Thomalla, F. (2003). "Resilience to natural hazards: How useful is this concept." *Environ. Haz.*, 5, 35–45.

Luers, A. L., and Lobell, D. B. (2003). "A method for quantifying vulnerability, applied to the agricultural system of the Yaqui Valley, Mexico." *Global Environ. Change*, 13, 255–267.

Mallak, L. (1998). "Putting organizational resilience to work." *Industrial Management.*, 40(6), 8–13.

McEntire, D. A. (2001). "Triggering agents, vulnerabilities and disaster reduction: Towards a holistic paradigm." *Disaster Prevention Management*, 10(3), 189–196.

Norman, S., Luthans, B., and Luthans, K. (2005). "The proposed contagion effect of hopeful leaders on the resilience of employees and organizations." *J. Leadership and Organizational Studies.*, 12(2), 55–65.

Ntuen, C. A., Balogun, O., Boyle, E., and Turner, A. (2006). "Supporting command and control training functions in the emergency management domain using cognitive systems engineering." *Ergonomics*, 49(12–13), 1415–1436.

Oomes, A. H. J. (2004). "Organization awareness in crisis management: Dynamic organigrams for more effective disaster response." *Proc., ISCRAM2004*, Brussels, Belgium, May 3–4, 63–68.

Pearson, C., and Mitroff, I. (1993). "From crisis prone to crisis prepared: A framework for crisis management." *Acad. Manage. Exec.*, 71, 48–59.

Pelling, M., and Uitto, J. I. (2001). "Small island developing states: Natural disaster vulnerability and global change." *Environ. Haz.*, 3, 49–62.

Penrose, J. M. (2000). "The role of perception in crisis planning." *Public Relations Review*, 26(2), 155–171.

Perrow, C. (1984). *Normal accidents, living with high-risk technologies*, Basic Books, New York.

Resilient Organizations (2006). "Program overview." ⟨http://www.resorgs.org.nz⟩ (January, 17, 2006).

Riolli, L., and Savicki, V. (2003). "Information system organizational resilience." *Omega, The International Journal of Management Science*, 31, 227–233.

Rognin, L., Salembier, P., and Zouinar, M. (2000). "Cooperation, reliability of sociotechnical systems and allocation of function." *Int. J. Hum.-Comput. Stud.*, 52, 357–379.

Roth, E. M., Multer, J., and Raslear, T. (2006). "Shared situation awareness as a contributer to high reliability performance in railroad operations." *Organ. Stud.*, 27(7), 967–987.

Runyan, R. C. (2006). "Small business in the face of crisis: Identifying barriers to recovery from a natural disaster." *J. Contingen. Crisis Manage.*, 14(1), 12–26.

Salmon, P., Stanton, N., Walker, G., and Green., D. (2006). "Situation awareness measurement: A review of applicability for C4i environments." *Appl. Ergon*, 37(2), 225–238.

Seaman, A. L., and Williams, J. (2005). "The perils of the plan." *CMA Management*, 79(1), 14–16.

Sheffi, Y. (2005). "Building a culture of flexibility." *World Trade*, 18(12), 26–29.

Sheffi, Y. (2006a). "Manage risk through resilience." *Chief Executive*, 214, 28–29.

Sheffi, Y. (2006b). "Waiting for the next 'big one.'" *Boston Globe*, Feb. 19, 11.

Smit, B., and Wandel, J. (2006). "Adaption, adaptive capacity, and vulnerability." *Global Environ. Change*, 16(3), 282–292.

Stanton, N. A., and Baber, C. (2006). "The ergonomics of command and control." *Ergonomics*, 49(12–13), 1131–1138.

Starr, R., Newfrock, J., and Delurey, M. (2004). "Enterprise resilience: Managing risk in the networked economy." *Strategy+Business*, 30, 1–10, ⟨http://www.bah.com⟩ (January, 30, 2005).

"The new penguin english dictionary." (2000). R. Allen, ed., Penguin Books, Harmondsworth, Middlesex, England.

Tierney, K. J. (1997). "Business impacts of the Northridge earthquake." *J. Contingen. Crisis Manage.*, 5(2),. 87–97.

Timmerman, P. (1981). *Vulnerability, resilience and the collapse of society. Environmental monograph 1*, Institute for Environmental Studies, Toronto Univ., Toronto, Canada.

Titan Systems Corporation (2002). "Arlington county after-action report on the response to the September 11 terrorist attacks on the pentagon." http://www.co.arlington.va.us/fire/edu/about/pdf/after_report.pdf (June 5, 2005).

Villagrán De León, J. C. (2006). "Vulnerability: A conceptual and methodological review." *Source No. 4/2006*, United Nations Univ. - Institute for Environmental and Human Security (UNU-EHS).

Walker, B. H., Gunderson, L. H., Kinzig, A. P., Folke, C., Carpenter, S. R., and Schultz, L. (2006). "A handful of heuristics and some propositions for understanding resilience in social-ecological systems." *Ecology and Society*, 11(1), 13, ⟨http://www.ecologyandsociety.org/vol11/iss1/art13⟩ (accessed January 11, 2007).

Watts, D. J. (2003). *Six degrees: The science of a connected age*, W. W. Norton, London.

Watts, M. J., and Bolhe, H. G. (1993). "The space of vulnerability: The causal factor in hunger and famine." *Progress in Human Geography*,

Nat. Hazards Rev. 2008.9:81-90.

17(1), 43–67.
Webb, G., Tierney, K., and Dahlhamer, J. (2003). "Predicting long-term business recovery from disaster: A comparison of the Loma Prieta earthquake and Hurricane Andrew." *Environ. Haz.*, 4(2–3), 45–58.
Weichselgartner, J. (2001). "Disaster mitigation: The concept of vulnerability revisited." *Disaster Prevention Management*, 10(2), 85–94.
Weick, K. E. (1993). "The collapse of sensemaking in organizations: The Mann Gulch disaster." *Adm. Sci. Q.*, 38(4), 628–652.
Weick, K. E., and Sutcliffe, K. M. (2001). *Managing the unexpected: Assuring high performance in an age of complexity*, Jossey-Bass, San Francisco.
Wellington Engineering Lifelines Group (WELG). (1994). "Section 1. Interdependence and response planning." Wellington Engineering Lifelines Group, New Zealand.

Nat. Hazards Rev. 2008.9:81-90.