The International Emergency Management Society
9th Annual Conference Proceedings
University of Waterloo, Canada, May 14-17, 2002

TEN THINGS YOUR ORGANIZATION CAN DO NOW

Geary W. Sikich

Principal, Logical Management Systems, Corp.

Key Words: Crisis, Continuity, Planning, Hazard, Vulnerability

Abstract

We are faced with a growing threat - ***terrorism***. The events of September 11, 2002 have forever changed the way we live. The security of the United States of America's infrastructure is a key concern of the White House. This presentation focuses on ten things that your organization can do now to improve survivability. Discussed are:

Ten Things Your Organization Can Do Now	
Action # 1	Make Your Enterprise an Unattractive Target
Action # 2	Revise Employee Screening Processes
Action # 3	Validate Business, Community and Government Contacts
Action # 4	Assess Business Continuity Plans
Action # 5	Train and Educate Your Workforce
Action # 6	Equip Your Workforce
Action # 7	Review leases and contracts for risk exposure
Action # 8	Assess value-chain exposure to supply disruptions
Action # 9	Review insurance policies and conduct cost/benefit analysis
Action # 10	Communicate Commitment

You need an open source for information on intelligence collection, data acquisition strategies directed against your company and its most valuable assets - your people.

Is your company prepared? Could an event, such as these, affect your company's existence?

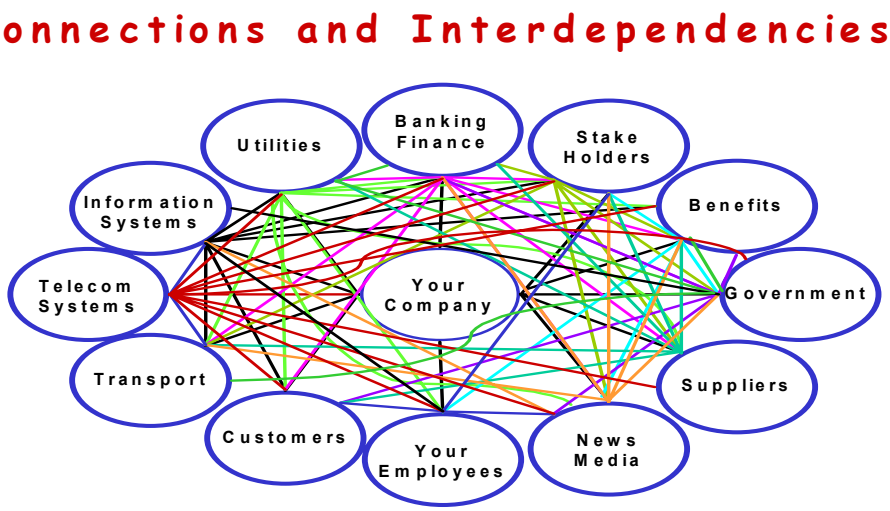
- Accidents, explosions, fires
- Natural disaster
- Environmental damage
- Product recall/tampering
- Workplace Violence
- Terrorism

Introduction

In the aftermath of the terrorist attack on the United States of America, the traditional rules governing the conduct of business are being obliterated as businesses are beginning to redefine how they will operate. The world was well on its way to blurring the distinction between traditional business and the appearance of widespread eBusiness operations. Products were

becoming services, services became products and business lines were changing constantly. As the authors of the book "*Blur*" state, "*Connectivity, Speed and Intangible Values are the new driving forces in business today. Traditional business boundaries are blurring as everyone becomes electronically connected*." Figure 1 below illustrates just how connected we are in today's world. With all this connectivity, you might ask yourself, "How resilient is my organization if our connectedness is interrupted?"

Figure 1: Connections and Interdependencies



Assumptions

The following assumptions have been made with regard to the recommendations contained in this white paper. First, events that have been building since the end of World War II, including thousands of terrorist attacks on innocent civilians worldwide, have culminated (so far) in vicious and indiscriminate attacks first by domestic terrorists and now by foreign terrorists on our homeland. Second, America is not immune from terrorism. Quite the contrary, we are a target rich environment for both domestic and international terrorists. The stakes are high, and the issues are indeed, life, death, and economic survival. Third, terrorists are driven to kill people and to destroy property. Fourth, all people and all facilities/operations are at risk. Fifth, priority terrorist targets are those of monetary or strategic value, having high human density and with cultural or symbolic value. Sixth, corporate headquarters of major corporations are prime targets. Seventh, most of what has to be done in the corporate environment must be done by the corporations themselves. Indeed, it is their responsibility to their people, their stockholders and to the public that relies on their products and services. Eighth, government, on the other hand, must concentrate its efforts on "critical infrastructures" such as electric power supplies, gas and oil, telecommunications, banking and finance, transportation, water supply systems, emergency services and continuity of government. Finally, corporate America must act now to make key assets (people, properties, equipment and information assets) unattractive targets for terrorists. Failure to do so is to be vulnerable to an attack.

In his book, "*6 Nightmares*", Anthony Lake relates the comments of World War II veterans, stating on page 92, "*…that battle was a struggle not just between two opposing armies but between two opposing ideas, and the qualities those ideas engendered in their respective fighting forces*." With

the events of September 11, 2001 The United States of America, its people and corporations have entered a new era of thought and belief. No longer are we able to ignore other ideologies and belief systems. We have created a global reach via the evolution of transcontinental travel, the Internet, communications media and business expansion worldwide. Our new global economy requires us to understand ideologies and beliefs. Nor will we ever be able to think that the trouble is "over there". Our challenge is to maximize the benefits of near instantaneous information while maintaining organizational structures that continue to be effective.

Crisis! Merely mention the word, and you evoke visions of unspeakable affliction and suffering. Recent events make those of the past, Three Mile Island, the Valdez oil spill, Bhopal, the Tylenol incident pale by comparison, and the list continues to grow. It seems that you can't turn on the radio or television or pick up a newspaper, magazine, or periodical any more, without reading about a crisis somewhere. Management is never put more strongly to the test than in a crisis situation. The objectives are immediate and the results have long term implications. Today, individuals responsible for the management of businesses and public agencies must be prepared to deal effectively with threats that could not be conceived of prior to September 11, 2001.

Ten Actions to Take Now

Government and Corporate America have long recognized the importance of being prepared. In the wake of many events, government passed regulations requiring Corporate America to develop and implement programs to assure preparedness. With the recent events we have experienced, can you wait until the government enacts new laws? The answer is no, Corporate America must take action now. Implementing the following seven actions within the context of your situation can produce positive results for your organization. The ***Ten Actions*** provided herein are presented in no order of precedence. You and your organization should assess their applicability and prioritize them as it fits your unique situation.

Ten Actions	
Action # 1	**Make Your Enterprise an Unattractive Target**
Action # 2	**Revise Employee Screening Processes**
Action # 3	**Validate Business, Community and Government Contacts**
Action # 4	**Assess Business Continuity Plans**
Action # 5	**Train and Educate Your Workforce**
Action # 6	**Equip Your Workforce**
Action # 7	**Review leases and contracts for risk exposure**
Action # 8	**Assess value-chain exposure to supply disruptions**
Action # 9	**Review insurance policies and conduct cost/benefit analysis**
Action # 10	**Communicate Commitment**

Action # 1 Make Your Enterprise an Unattractive Target

Making your enterprise an unattractive target is one of the basic tenants of security, as well as, business continuity preparedness. Whether it is a terrorist or a criminal, if your enterprise presents significant barriers to access it is less likely to be targeted. The application of active security measures, as well as, passive security measures serves to deter the perpetrator to another target. For example, you may wish to change your security personnel's uniforms in order to make them more visible. A simple change like this can have an effect by making people more aware of the presence of the security personnel. You can introduce "Target Hardening" measures, such as, decorative concrete barriers, cameras, perimeter lighting and access badges. These measures act as passive deterrents to unauthorized entry. You can also add barriers to access, such as, manned

guard emplacements with gates, tire spikes, reinforced fencing and the removal of vegetation and next to building parking areas.

Action # 2 Revise Employee Screening Processes

Do you really know who your employees are? Are you sure that the person you hire has represented their background honestly? Taking this action may assist you and your organization solve a very real problem, "How do I know?" More than ever, employers need to identify employees and potential employees who are at risk of being exploited, compromised and/or co-opted, by terrorists or criminals for information, access and/or passive cooperation. The better you know your employees, the less likely your organization presents a target. You can accomplish this through implementing a system of more detailed background investigations designed to provide assurance of the information provided to your organization.

Implementing a system of checks and balances whereby critical information and/or access is not subject to compromise can also afford your organization more security. A "Workplace Violence" program is also useful for diffusing potential conflict situations. Employee Assistance programs should be reviewed and assessed for effectiveness and for accessibility by your personnel.

Action # 3 Validate Business, Community and Government Contacts

The more you know about the support services that you depend on and your organization's linkages to suppliers, customers and dependencies on critical infrastructures the less apt your enterprise will be to assume too much. You should learn as much as you can about the Critical Infrastructures your enterprise depends on, including electric power supplies, gas and oil, telecommunications, banking and finance, transportation, water supply systems, emergency services and continuity of government.

In addition to learning about and planning for Critical Infrastructure disruptions, your organization should get to know about the expectations and capabilities of your suppliers, business partners and customers. For example, how would you deal with a situation in which one of your critical suppliers was not able to meet a scheduled delivery? Or what if a customer had an event and could not occupy their facilities? Would your organization be able to coordinate with the supplier or customer to the mutual satisfaction of all parties?

Action # 4 Assess Business Continuity Plans

Does your organization's current approach to business continuity employ an "All Hazards" approach or are your plans segmented into a series of plans that are not integrated? A key question you may wish to ask yourself is, "Does our current Business Continuity Plan address all the threats that face our organization?" If your Business Continuity Plan is focused on only a portion of your organization, such as information systems disaster recovery, you may want to rethink and rework your plans into an "All Hazards" plan. An assessment of your program against the "All Hazards" approach may be the answer to uncertainty. An "All Hazards" plan will take into consideration life safety issues, emergency response, event management, operational events, workplace relocation and external events that can have a negative impact on your organization.

When broken down into its basic elements, the "All Hazards" approach consists of only six parts: preparation and prevention; detection and classification; response and mitigation; reentry, recovery and resumption; training and resource development; and information management.

Although no two business continuity programs are exactly alike, the above six elements form the critical aspects of the "All Hazards" approach to business continuity planning.

Action # 5 Train and Educate Your Workforce

A trained and educated workforce can do more to protect your enterprise than you can imagine. Training of personnel is a critical component of the "All Hazards" approach to business continuity planning and preparedness. Training your personnel at all levels is one of the critical success factors that must be addressed if an adequate response to an event is to be achieved. A "systems" approach to preparing effective training programs should consist of:

- ***Task analysis****:* When designing an integrated training program, first determine the skills, knowledge, and procedures required for satisfactory performance of each task.
- ***Lesson Development****:* Learning objectives are defined from the skills, knowledge, and procedures developed during task analysis. Instructional plans are then prepared to support the learning objectives.
- ***Instruction****:* Lessons are systematically presented using appropriate instructional methods. Instruction may include lecture, self-paced or group-paced mediated instruction, simulation and team training.
- ***Evaluation****:* Performance standards and evaluation criteria are developed from the learning objectives. Each trainee's performance is evaluated during the course and during field-performance testing.

In addition to formal training programs, a program of proficiency demonstration to validate the training and content of plans is also needed. This can be accomplished by establishing a program that supplements the training with simulations (drills and exercises).

Consider developing programs to educate your employees on basic life safety (first aid, CPR, Evacuation, Assembly, Accountability), what to do if an event occurs and what to do after the event. In addition, a community outreach program can provide your organization with many benefits. A community outreach program can enhance coordination with local emergency response and law enforcement agencies, put your organization in a positive light in the community and provide your employees more information on community resources.

Action # 6 Equip Your Workforce

You cannot stop at classroom training and expect your organization to respond effectively to an event. Corporate America needs to assess how prepared it is to deal with workplace events. The government must focus its attention on the protection of critical infrastructures and international issues.

Corporate America has to address protective measures that ensure its survival; it cannot depend blindly on the government to be there for assistance. Being able to respond appropriately will be essential, however, responding without the proper equipment can lead to failure. You need to equip your workforce with the appropriate emergency response equipment, such as: first aid kits, fire extinguishers, event response kits, and evacuation, assembly, accountability procedures.

You should also understand that when you purchase the equipment and train your personnel on its use, you have to develop and implement a maintenance program to assure that the equipment is there and that it works when it is needed.

Action # 7 Review leases and contracts for risk exposure

Every organization needs to completely assess its risk exposure. This includes the standard risk exposure methodologies currently employed by your organization. In addition to the standard risk assessment methodologies, however, your organization should review all leases and contracts for potential risk exposure specifically addressing the issue of terrorism and terrorism related events. As

described in item # 8, LMS' "CARVER Analysis" system provides an integrated approach to determining risk exposures.

Action # 8 Assess value-chain exposure to supply disruptions

Critical to all organizations is their value chain. The value chain includes all the internal external "touch points" to suppliers, customers, outsourcing, strategic partners and other entities that assure your organization's continued success. As with the critical infrastructure assessments, your organization needs to assess the potential effects of a disruption of its value chain to supply disruptions. In conducting the assessment a variety of scenarios need to be developed to assess the short term, intermediate term and long term effects of a disruption. This assessment should consider the following key factors as depicted in the table below, entitled, "LMS' CARVER Analysis Elements." The first element is "Criticality". A determination as to the criticality of the service, product, etc. being supplied via the value chain is essential, if you are going to adequately assess the potential risk exposure. Once criticality is established, an assessment of "Accessibility" is necessary. By "Accessibility" I am referring to how accessible an item is.

One needs to assess the accessibility to the item, the accessibility to alternative items that can be substituted and the accessibility of the item to disruption. Once "Criticality" and "Accessibility" are established, you need to determine "Recognizability". That is, how readily recognizable is the item with respect to its loss from your organization's value chain. If I am targeting your organization, I am going to look at readily recognizable items that can be accessed and are critical to your operations. Once the first three items' weighting parameters are established, one must determine the "Vulnerability" presented by the potential loss of the element in your value chain. For example; let's say you are a distributor and are concerned over critical inventory. While your information systems may be able to accurately depict your inventory, if you were to lose access to your inventory supply location or ability to move the inventory to market it would not matter how accurately you could determine the level of inventory, as you and your customers would not be able to access the items. A "Vulnerability" can therefore be defined as a the potential for any degradation, interruption or non-recoverability to such an extent that the consequence is likely to result in harm to the organization, harm to others (suppliers, customers, etc.) and/or substantial negative financial impact. A "Vulnerability", therefore, can arise from a: false ASSUMPTION; blocked or altered COMPONENT; blocked or altered FUNCTION; or blocked or altered OPERATION.

Once you have established, "Criticality", "Accessibility", Recognizability and "Vulnerability" you must determine the "Effect" of the loss of the value chain item. "Effect" can and will generally be associated to the impact of the loss. However, one must consider all aspects of "Effect", there can and may be some positive "Effect" that can arise from the loss or interdiction of the value chain. Lastly, one must determine the "Recouperability" aspects associated with the potential loss or disruption. How resilient is my organization? Can we quickly respond to, manage and recover from a disruption of the value chain? The net result of conducting a "CARVER Analysis" is to be able to determine the potential significance of an event from a consequence management perspective.

Table 1: LMS' CARVER Analysis Elements

LMS' CARVER Analysis Elements
C = **Criticality**
A = Accessibility
R = Recognizability
V = Vulnerability
E = Effect
R = Recouperability

Action # 9 Review insurance policies and conduct cost/benefit analysis

As a result of the events that occurred on September 11, 2001 and subsequent events taking place now, a review of insurance policies with respect to coverage, exclusions and exceptions needs to be accomplished. Insurance companies have been and will be impacted by the events of September 11th and events yet to occur.

Many organizations will find that a cost benefit analysis will offer an effective aid to decision making, strategy planning and the development of risk reduction solutions. By applying LMS' "CARVER Analysis" tool to the evaluation, cost/benefit analysis can be finely tuned to reflect a clearer picture of true costs and benefits. Changes in insurance coverage for many organizations in what are deemed to be high risk/high exposure areas will potentially cause a financial burden for many organizations. This could lead to adverse effects on the organization's ability to maintain its business orientation, retain and/or increase staff and continue to operate from current domicile locations.

Action # 10 Communicate Commitment

Without the support of the entire enterprise all the preparation and planning, all the equipment and training, all of the liaison and information sharing will go for naught. From the highest level to the lowest, everyone in your organization must be kept well informed. Information is a corporate asset, and it's expensive. It must be shared and managed effectively. Information management is also critical during an event. The need for active systems to provide information on materials, personnel, capabilities and processes is essential. It is extremely important to have a system and adequate backup systems in place that serves to identify, catalog, prioritize, and track issues and commitments relating to event management and response activities.

The need to communicate commitment throughout the organization on an ongoing basis is also very important. If your personnel feel that you are only giving lip service to preparedness they are soon going to develop a lax attitude toward preparedness.

Communicating commitment is an ongoing dynamic process that is cyclical and must be supported and actively worked on by all levels of the organization. Active participation can ensure operational resilience. The process doesn't end just because you finished your plan, have involved management and have trained the staff.

Conclusion

Trust and confidence in the abilities of all levels within your organization must be established. "How well prepared are we?" This question can only be answered satisfactorily if you have established a level of trust and confidence, can communicate risk and are willing to allow your people to practice upward management — to delegate up. They must have the ability to recognize needs and have a process in place that allows them to delegate up without fear of repercussions.

You can ensure that all levels within the organization are involved in preparedness. This can be achieved in several ways. The first is to establish a formal program and assign the program to a senior manager directly responsible to top management and the board of directors. Second, establish performance measurements throughout your organization that incorporate an evaluation of preparedness. This goes both ways. Upper management has to take responsibility for developing measurable and attainable goals for the organization to achieve. Third, set aside a specific time for reports on preparedness (business continuity and operational resilience) issues. This can be accomplished by preparing an agenda for senior staff and board of directors' meetings that includes a discussion of management preparedness as a mandatory item. You have to give it more than lip service, though, and you must make the discussion substantive. Provide more than the dull and tiring statistics on reportable accidents, etc. Include all levels of personnel in the presentation

process. This can be very effective, and it gets the message out to all personnel that your organization is serious about its preparedness. Fourth, make preparedness issues part of the strategic planning process and a component of your competitive analysis activities. Making preparedness a part of the way you do business, instead of an adjunct to the business is critical. Finally, communicate the information on the importance of preparedness through all levels of your enterprise. This can be accomplished through formal adoption of policy at the highest levels of the organization. The board of directors should endorse your preparedness actions.

References:

"September 11 Aftermath: Seven Things Your Organization Can Do Now", published in Disaster Recovery Journal, Winter 2002, Volume 15, Number 1

"September 11 Aftermath: Ten Things Your Organization Can Do Now", John Liner Review, Winter 2002, Volume 15, Number 4.

Davis, Stanley M., and Christopher Meyer, *Blur: The Speed of Change in the Connected Economy* (Boston: Addison-Wesley, 1998).

Lake, Anthony, *"6 Nightmares, Real threats in a Dangerous World and How America Can Meet Them"*

"It Can't Happen Here: All Hazards Crisis Management Planning", Geary W. Sikich, PennWell Publishing 1993.

"The Emergency Management Planning Handbook", Geary Sikich, McGraw Hill, 1995.

Critical Infrastructure Vulnerability - An Overview of the Findings of the President's Committee on Critical Infrastructure Protection, Geary Sikich, Independent Liquid Terminals Association '98, 1998.

Managing Crisis at the Speed of Light: The Transition to the Next Millennium, Geary Sikich, Aircraft Handling Expert Magazine, 1999

Business Continuity & Crisis Management in the Internet/E-Business Era, Geary Sikich, Teltech, 2000

Author Biography

Geary W. Sikich gsikich@aol.com is the author of ***It Can't Happen Here: All Hazards Crisis Management Planning*** (Tulsa, Oklahoma: PennWell Books, 1993) and the ***Emergency Management Planning Handbook*** (New York: McGraw-Hill, 1995), available in English and Spanish-language versions. Mr. Sikich is the founder and a Principal with Logical Management Systems, Corp., based in Munster, IN. He has over 20 years experience in management consulting in a variety of fields. Sikich consults on a regular basis with companies worldwide on business continuity and crisis management issues. He has a Bachelor of Science degree in criminology from Indiana State University and Master of Education in counseling and guidance from the University of Texas, El Paso. Since its inception in 1985, Logical Management Systems, Corp. believes that a strategic approach to event management, involving careful analysis can help to avoid problems and transform issues into opportunities. We have helped many organizations develop and implement effective event management programs. www.logicalmanagement.com