"Futureproofing" - the Process of Active Analysis

By Geary W. Sikich

Overview

The ability to effectively respond to and manage the consequences of an event in a timely manner is essential to ensure an organization's survivability in today's fast paced business environment. With the emergence of new threats, such as cyber-terrorism and bio-terrorism; and the increasing exposure of companies to traditional threats such as, fraud, systems failure, fire, explosions, spills, natural disasters, etc. an "*integrated*" approach to Business Continuity Planning is essential. The "*integrated*" approach, as presented in this article, is based on the concept of graceful degradation and agile restoration. "G*raceful degradation*" refers to the ability of an organization to identify the event, classify it into a level of severity, determine its consequences, establish minimal stable functionality, devolve to the most robust less functional configuration available and to begin to direct initial efforts for rapid restoration of services in a timely fashion.

Hazard, Threat, Risk, Vulnerability and Consequence Analysis

Most organizations employ a business impact assessment as the initial step to developing their business continuity plan. The following matrix summarizes the typical matrix of events that are assessed.

Risks/Threats/Hazards/Vulnerabilities Potential Events	Probability (H,M,L)	Impact (H,M,L)	Effect (LT, ST)
Bomb Threat			
Bomb Event			
Customer Injury on Premises			
Data Entry Threat/Employee Error			
Disruption of Courier/Mail Delivery Service			
Earthquake			
Executive Succession			
Explosion			
Fire			
Fraud/Embezzlement			
Health Event (Employee Life Safety)			
Heating/Cooling Failure			
Hurricane			
Kidnapping/Extortion			
Lightning			
Loss of Critical Personnel			
Natural Gas Leak/Carbon Monoxide			
Power Failure			
Robbery/Assault			
Severe Weather Conditions			

Snow/Ice			
Software Failure/Virus			
Tampering with Sensitive Data			
Telecommunications Failure			
Terrorist Act			
Tornado/Wind Damage			
Unauthorized Access/Vandalism			
Water Damage/Rain Storms			
Weapons of Mass Disruption (Chem/Bio)			
Weapons of Mass Destruction (WMD)			
Workplace Violence			
Additional Vulnerabilities not listed here			

Additional vulnerabilities listed generally do not account for external vulnerabilities that may remain unidentified by the organization until an event occurs and they are affected by it.

Traditional analysis such as that performed at the initiation of the business continuity plan development is recognized as necessary to develop a baseline of information. However, it should also be recognized as having certain limitations:

- *Pre-Event - Best guess as to what could occur*
- *Static - Best guess based on available facts and models*

Traditional analysis creates undecidability due to the inability to predict all behavior in a dynamic environment. Therefore one should adopt an *Active Analysis* methodology, such as that developed by Logical Management Systems, Corp. (LMS). LMS' methodology is based on the U.S. Military's "Joint Special Operations Targeting and Mission Planning Procedures" (JP 3-05.5 10 august 1993). It is detailed herein.

The advantages that can be realized by adopting this methodology and maintaining an active analysis process are:

- *Uses Static Analysis as a basis*
- *Touchpoint complexity factors*
- *Dynamic - based on creating a mosaic*
- *Time Factors (Time Critical, Time Sensitive and Time Dependent) act as drivers*

Termed "*Futureproofing*" by LMS the active analysis process is designed to create a mosaic that enhances decision making by identifying behavior patterns in a dynamic environment.

Active analysis can be subdivided into three categories of possible threats/occurrences that could befall an organization. Dr. Ian Mitroff refers to the three categories as Natural Accidents, Normal Accidents and Abnormal Accidents. I have renamed them and to differentiate the three aspects of each. That is, the threat, the actual occurrence and the consequence of the occurrence.

- **Natural Threats/Occurrences/Consequences** consisting of such things as drought, floods, tornadoes, earthquakes, fires and other naturally occurring phenomena.

- **Normal Threats/Occurrences/Consequences** consisting of such things as Economic Disasters, such as:

    - Recessions
    - Stock Market Downturns
    - Rating Agency Downgrade, etc.

  Personnel Disasters, such as:

    - Strikes
    - Workplace Violence
    - Vandalism
    - Employee Fraud, etc.

  Physical Disasters, such as:

    - Industrial Accidents
    - Supply Chain
    - Value Chain
    - Product Failure
    - Fires
    - Environmental
    - Health & Safety

- **Abnormal Threats/Occurrences/Consequences** consisting of Criminal Disasters, such as:

    - Product Tampering
    - Terrorism
    - Kidnapping & Hostages, etc.

Information Disasters, such as:

- Theft of Proprietary Information
- Hacking, Data Tampering
- Cyber Attacks, etc.

Reputation Disasters, such as:

- Rumors
- Regulatory Issues
- Litigation
- Product Liability
- Media Investigations
- Internet Reputation, etc.

Please note Abnormal Threats/Occurrences/Consequences are becoming more of the norm than abnormal as we see the normalization of threats such as hacking and data tampering.

Five key assumptions were used as a basis to for the developmental framework of the "*Futureproofing*" methodology. These are:

- **Assumption # 1**: The modern business organization represents a complex system operating within multiple networks

- **Assumption # 2**: There are many layers of complexity within an organization and its "Value Chain"

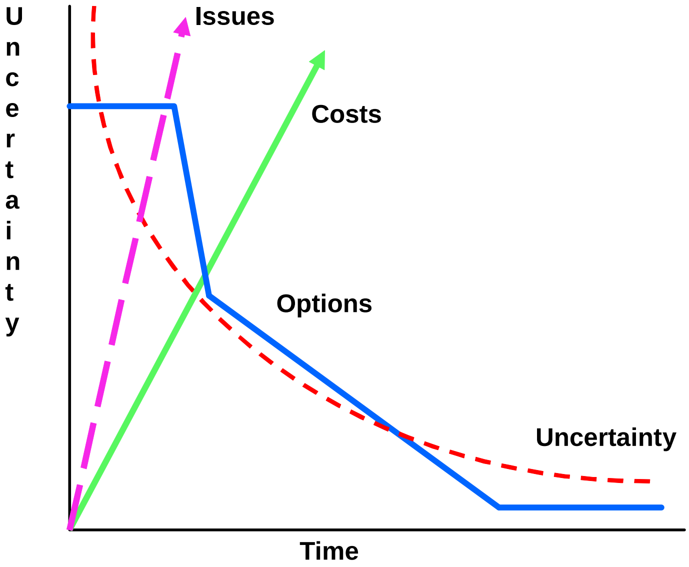
- **Assumption # 3**: Due to complexity, active analysis of the potential consequences of disruptive events is critical

- **Assumption # 4**: Actions in response to disruptive events needs to be coordinated

- **Assumption # 5**: Resources and skill sets are key issues

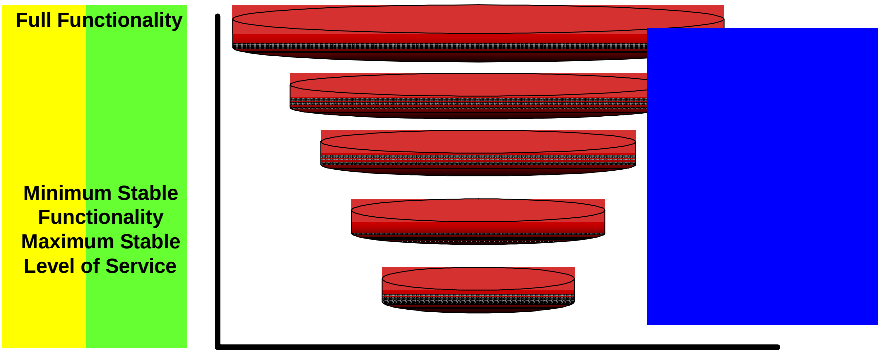
Based on the above assumptions and the results of the baseline analysis (static analysis) one realizes that the timely identification, classification, communication and response, management and recovery from a disruptive event are critical. As depicted in the graphic on the next page over time uncertainty will decrease, as will available options for response and recovery.

This is contrasted with increasing numbers of issues and higher and higher costs associated with response and recovery efforts. As such, an organization should seek to continually analyze situations so as to develop a clear picture of the current state of the business system network. Referred to as "Data Fusion - *Constructing a Mosaic*" by LMS; this is a process of getting enough bits and pieces of information in place in order to transform seeming chaos into recognizable patterns upon which decisions can be made.



The strategy for "graceful degradation and agile restoration" is depicted in the graphic below.

Graceful Degradation + Agile Restoration = *Resilience*


Full Functionality
Minimum Stable Functionality Maximum Stable Level of Service

Devolve to most robust less functional configuration

(Time, Services)

Where the outer ring represents the business system and its network in full functionality. The inner broken line rings represent successive levels of "graceful degradation" that the business system and its network will undergo until reaching a level of minimum functionality. When the business system and its network reaches the state of minimum functionality, the organization can begin to conduct a campaign of "agile restoration" until it achieves a state of full functionality and a return to normal operations. One key to the process of "graceful degradation and agile restoration" is having a classification system for the Business Continuity Plan. As the graphic below depicts, "detectors and indicators of change" are employed to facilitate the constant analysis of the state of the business system and its complex "value chain" network. The "detectors and indicators of change" provide the early warning basis for event classification at the lowest (least severe) levels.

Business Impacts Matrix

Depicted below is an example of a business impact matrix that can be developed as part of a worksheet for active analysis. The matrix represents the critical elements within the business system's network that, if interdicted, would pose a threat to the business system's ability to conduct normal business operations. The elements considered are as follows:

- **Personnel** - consisting of management, employees, stakeholders, suppliers, providers, partners, contract/vendor entities, etc.

- **Clients** - consisting of current, new and former customers.

- **Systems** - consisting of internal operating systems and critical external infrastructures.

- **Suppliers** - consisting of providers of essential business logistics.

- **Utilities** - consisting of electric, gas, water and telephone service providers

- **Water** - consisting of water treatment and other water support systems.

- **Telecommunications** - consisting of internal telecommunications systems linked to external telecommunications providers.

- **Energy Supply** - consisting of energy delivery systems and energy support systems.

- **Government Services** - consisting of emergency management, police, fire, emergency medical, Federal, State and local government bodies and political support systems.

- **Transportation** - consisting of air, land and water transportation system and support systems.

- **Financial Services** - consisting of financial markets, investments, statutory deposit requirements and cash flow systems.

Each of these elements is periodically rated as part of the Active Analysis system to determine the potential impact of loss or degradation on the business system and its network.

A simple ranking methodology utilizing High, Medium and Low (H, M, L,) designations can provide a basis for determining situational loss or degradation effects. The matrix below provides an example of such an analysis.

Business Impacts Matrix	PERSONNEL	CLIENTS	SYSTEMS	SUPPLIERS	UTILITIES	WATER	TELECOMMUNICATAONS	ENERGY SUPPLY	GOVERNMENT SERVICES	TRANSPORTATION	FINANCIAL SERVICES
Corporate Office	L	H	H	H	H	M	M	M	M	L	M
Business Unit #1	M	H	H	M	H	M	M	M	L	M	L
Business Unit #2	M	M	M	L	M	M	H	M	L	M	L
Business Unit #3	L	M	M	L	M	M	H	M	L	L	L
Business Unit #4	L	M	M	L	M	M	H	M	L	L	L
Business Unit #5	L	M	M	L	M	M	H	M	L	L	L
Business Unit #6	L	M	L	L	M	M	H	M	L	L	L
Business Unit #7	L	M	M	L	M	M	H	M	L	L	L

Active Analysis Methodology

The following section is a discussion of the "Active Analysis" system employed by Logical Management Systems, Corp. Based on the ***LMSCARVER*****^{TM}** Analysis Elements, the system provides a flexible framework for the continuous accumulation and assessment of "detectors and indicators" of change. As defined below these are the key elements:

“**Critical**”: Determine the criticality of the service, product, etc. that the business system and its network utilize. This may be supplied via the network value chain or an external entity.

“**Accessible**”: Determine “Accessibility” by ranking the element as to the ease with which someone can access the element. 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.

“**Recognizable**”: Determine how readily recognizable the element is.

"**Vulnerable**": Determine the total loss and/or degree of degradation that the organization can sustain. A “Vulnerability” can arise from a:

- false ASSUMPTION;
- blocked or altered COMPONENT;
- blocked or altered FUNCTION; or
- blocked or altered OPERATION

“**Effect**” Determine what impact the loss and/or degradation presents to your organization.

“**Recoverable**” Determine what your organization's recovery ability is.

Recovery Time Objective (RTO): Anticipated time to recover operation.

Recovery Point Objective (RPO): Amount of loss that can be sustained without impact to operation.

Directions: The form below is designed to facilitate the evaluation of risks, threats, hazards and vulnerabilities and to determine the consequences of touchpoint degradation to the business system and its network. Choose a touchpoint from part 1 for analysis. Insert the named touchpoint into the area of analysis box in Part 2 and complete the CARVER analysis ranking the touchpoint using the numeric rating system. Complete Part 3 by filling in the consequence management significance to the business system and its network.

LMSCARVER^{TM} Analysis - Business Continuity Touchpoint Assessment Form

PART 1: ORGANIZATION TOUCHPOINTS

✓	Touchpoint	✓	Touchpoint
	Electric Power Supplies		Internal Systems
	Gas and Oil Systems		Facilities
	Telecommunications Systems		Equipment
	Banking and Finance Systems		Human Resources Key Personnel
	Transportation Systems		Human Resources Staff Elements
	Water Supply Systems		Suppliers
	Emergency Services		Customers
	Continuity of Government Services		Contract Services (specify)
	Corporate Image		Stakeholders (specify)
	Operational Infrastructure (specify)		Other (specify)

PART 2: TOUCHPOINT ANALYSIS

Area of Analysis:	Lowest			Highest		Comments
	1	2	3	4	5	Recovery Time Objective Recovery Point Objective
C = Critical						
A = Accessible						
R = Recognizable						
V = Vulnerable						
E = Effect						
R = Recoverable						
Totals						

PART 3: CONSQUENCE MANAGEMENT SIGNIFICANCE

Conclusion: Seize the Initiative - It Makes Sense

A Chinese proverb states that "*Opportunity is always present in the midst of crisis*." Every crisis carries two elements, danger and opportunity. No matter the difficulty of the circumstances, no matter how dangerous the situation… at the heart of each crisis lies a tremendous opportunity. Great blessings lie ahead for the one who knows the secret of finding the opportunity within each crisis.

Today business leaders have the responsibility to protect their organizations by facilitating continuity planning and preparedness efforts. Using their status as “leaders,” senior management and board members can and must deliver the message that survivability depends on being able to find the opportunity within the crisis.

Many people feel that the world has changed as a result of the events that took place on September 11, 2001; that we need to rethink our concepts of continuity and crisis management. Today we cannot merely think about the plannable or plan for the unthinkable, but we must learn to think about the unplannable.

Market research indicates that only a small portion (5%) of businesses today have a viable plan, but virtually 100% now realize they are at risk. Seizing the initiative and getting involved in all the phases of crisis management can mitigate or prevent major losses. Just being able to identify the legal pitfalls for the organization of conducting a crisis management audit: can have positive results.

About the Author

Geary W. Sikich is the author of "*It Can't Happen Here: All Hazards Crisis Management Planning"* (Tulsa, Oklahoma: PennWell Books, 1993). His second book, "*Emergency Management Planning Handbook"* (New York: McGraw-Hill, 1995) is available in English and Spanish-language versions. His third book, "*Integrated Business Continuity: Maintaining Resilience in Uncertain Times*," (PennWell 2003) is available on www.Amazon.com. Mr. Sikich is the founder and a principal with Logical Management Systems, Corp. (www.logicalmanagement.com), based in Munster, IN. He has extensive 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.