

Integrated Business Continuity: Maintaining Resilience in Uncertain Times

By Geary W. Sikich





Table of Contents

List of Figures	ix
List of Tables	xi
List of Acronyms	xv
Foreword	xvii
Chapter 1	
Entering the Age of Uncertainty: What to Expect	1
Chapter 2	
Critical Infrastructures: Opportunities and Vulnerabilities	17
Chapter 3	
The Underpinnings of Business Continuity	47
Chapter 4	
Your Next “Crisis:” Identifying Time-Critical Issues	79
Chapter 5	
The Smoldering “Crisis:” Time-Sensitive Issues	97
Chapter 6	
The Hibernating “Crisis:” Time-Dependent Issues	111
Chapter 7	
Business Continuity: From Inception to Integration	125
Chapter 8	
Protecting Your Organization in the Age of Uncertainty	151
Chapter 9	
Knowledge Management: Effective Com- munications in the “Age of the Instant”	167
Chapter 10	
The Next Wave: Global Vulnerabilities, Local Impacts	181
Chapter 11	
Concluding Thoughts	207
About the Author	227
Index	229



List of Figures

1-1	Connections and Interdependencies	3
1-2	Basic Assumptions	5
2-1	LMSCARVER™ Analysis Elements	30
3-1	Business Continuity: Common Elements	51
3-2	Organizational Silos	52
3-3	Strategy	56
3-4	Competitive Intelligence	57
3-5	Event Management	59
3-6	Four Pillars of Business Continuity	62
4-1	Where's Your Next Event Coming From?	81
10-1	Worst-Case Scenario	190
10-2	Most-Likely-Case Scenario	190
10-3	Best-Case Scenario	191
11-1	Time-Critical, Time-Sensitive, Time-Dependent	213
11-2	Expectations—Agenda—Focus	215
11-3	Six Key Questions	216
11-4	Data Fusion	217

List of Tables

1-1	Long- and Short-Term Threat Trend Assessment	9
2-1	Time-Critical, Time-Sensitive, Time-Dependent Equations	31
2-2	Consequence Management—Cascade Effect	32
2-3	Phases of Event Response and Typical Activities	33
2-4	10 Things Your Organization Can Do Now	41
2-5	Heightened Concerns...	42
2-6	...and Greater Precautions	43
3-1	Business Decision-Making and Decision-Application	60
3-2	Does This Describe Your Enterprise?	61
3-3	Decision-Making Model	67
3-4	Disaster Exposure Rating Chart	68
3-5	Certified Knowledge Engineer	70
3-6	Essential Elements of Analysis: Example Assessment	75
4-1	Time-Critical Event Survey	82
4-2	Business Continuity Quiz—Time-Critical Issues	84
4-3	Answer Form	85
4-4	Strategy, Competitive Intelligence, and Event Management	86
4-5	Assigning Responsibility for Business Continuity Processes	87
4-6	Events That Could Occur to Any Organization	89
4-7	Possible Time-Critical Situations—Probability of Occurrence	90
4-8	Possible Time-Critical Situations—Impact on the Business	91
4-9	Highest Priority Time Critical Situations— Most Likely and Greatest Impact	92
4-10	How to Address a Time-Critical Event	93
4-11	Thinking Through Development of Time-Critical Elements	94
5-1	Time-Sensitive Event Survey	99
5-2	Business Continuity Quiz—Time-Sensitive Issues	101
5-3	Scoring	102
5-4	Events That Could Occur to Any Organization	103
5-5	Possible Time-Sensitive Situations—Probability of Occurrence	104

8-1	Assessing Current Competitive Intelligence Vulnerabilities	155
8-2	10 Actions	158
9-1	Need to Know vs. Nice to Know	173
10-1	Workplace Violence Scenario Information Sequence #1	185
10-2	Workplace Violence Scenario Information Sequence #2	186
10-3	Workplace Violence Scenario Information Sequence #3	187
10-4	Workplace Violence Scenario Information Sequence #4	188
10-5	Workplace Violence Scenario Information Sequence #5	189
10-6	Assessing Events by Organization Sector	195
10-7	Lessons from an Event Apparently Unrelated to Your Business Sector	197
10-8	Global Vulnerabilities—Local Impacts	202
11-1	Board Responsibility by Selected Countries	220
11-2	How Often Are Business Continuity Issues Referred to the Board?	222



Foreword

MANAGING YOUR NEXT “CRISIS” AT THE SPEED OF...?

As the authors of *Blur* point out:

Connectivity, speed and intangible values are the new driving forces in business today. Traditional business boundaries are blurring as everyone becomes electronically connected. The traditional rules governing the conduct of business are blurred as businesses are redefined, products become services, services become products and business lines change constantly.

As business change accelerates, it is getting more and more difficult for traditional strategists to achieve an accurate focus on the current situation. Strategy, in the traditional sense, is outdated before it can be implemented. Speed, operating at real time, is pushing traditional strategy development, forecasting, competitive intelligence collection, and analysis to new limits. For every organization, vision, mission, and values are important; they shape strategy for the organization. Strategy, in turn, is influenced by information in the form of competitive intelligence; competitive intelligence initiatives seek to fulfill a company's strategy. Due to the speed of business in the modern organization today, “crises” (disruptive events) are prevalent. Every “crisis” is a violation of vision, mission, and values. Every crisis solution demands a modification, if not wholesale reworking, of strategy (vision, mission, values) and competitive intelligence activities. As the strategy and competitive intelligence disciplines come under more scrutiny, the need for a comprehensive event management system becomes paramount. The integration of strategy, competitive intelligence, and event management into a vertically and horizontally seamless process allows for “integrated” business continuity.

An effective and well adhered-to “integrated” business continuity management system provides value for the organization, by allowing it to adapt to the rapidly changing business environment we are faced with today. The speed of response to an event will determine the outcome, either positive or negative, for the organization and its value chain. The ability to connect all the touch-points within an organization and its value chain during an event is essential for the success of response, management, and recovery efforts. The value achieved through an organized response, management, and recovery effort to a disruptive event is measured by the intangibles—perception, information,

relationships, and loyalty. These cannot be seen, and often it is difficult to measure their impact.

All organizations plan for business success, yet few plan for the potentially devastating effects of an event that becomes a “crisis”. Fewer still know and understand the critical process of knowledge management. “Crises” can take many forms; being prepared can be the most effective tool you can employ to assure that your business survives. Where’s your next event that has potential for becoming a “crisis” coming from? Will it be a time-critical issue that demands immediate action? Will it be a time-sensitive issue that, if not addressed, will erupt into a full-blown “crisis”? Or will it be a time-dependent issue that lingers unnoticed until it’s too late to react effectively? No one plans to have a business disruption; we plan for business growth and success.

Disruptive events, small and large, don’t make appointments; they can and do occur at any time and under the most unfavorable conditions. You can, however, prepare your organization, have in place early warning systems, and minimize the potential disruption to your business, your life, and your community, by adopting and developing a proactive business continuity process. Incorporating your business continuity process into the way you do business instead of as an adjunct to the business that your organization does can further ensure that your enterprise will be around after an event, instead of as a footnote to the event.

With the tragic events that occurred on Sept. 11, 2001 in New York City, Washington, D.C., and in a field in Pennsylvania, the need to address business survivability in a “new threat environment” has gotten a lot of press. However, is it truly a “new threat environment”? Have we not had the threat of terrorism and acts of violence facing society for some time? The obvious answer is yes, we have. What changed, as a result of Sept. 11, 2001, was not the nature of the threat, but the magnitude. It came to our shores and it occurred on a scale that few could have imagined. We now have many who predict such dire events as a nuclear attack, or chemical and biological attacks, that may affect millions. While these dire predictions may come to pass (hopefully, not), there are things that can be done to lessen the effect and possibly mitigate the event before it occurs. I, therefore, have based much of this book on the following assumptions.

COMPLEXITY—NETWORKS—TOUCHPOINTS

My assumptions for this book, while focusing on business, can be applied to other entities, including government. As such, I have taken the liberty to use the term “business” in the broadest sense of the word and will entrust

the reader to substitute the appropriate terminology as applicable when the word “business” is used.

The term “business continuity” as used in this text will refer to an integrated process that combines—

- “life safety” (emergency preparedness, emergency response)
- “disaster recovery” (information/data recovery)
- “business resumption” (facilities/operations recovery)
- “crisis management” (internal/external communications, issues management) under the term
- “event management.” Event management is combined with strategy and competitive intelligence initiatives to create an “integrated” approach to business continuity.

I use the term *business continuity* as an integrated approach, based on common terminology, detailed assessment of relationships/touchpoints and integrated response, management, recovery, and information-sharing processes. This integrated process is based on a careful identification, analysis, assessment, and prioritization of the organization’s ability to reduce its activities until it reaches stability and to maintain stability as it adds back activities. I will use the terms *graceful degradation* and *agile restoration* throughout this text as I investigate the business continuity process.

By *graceful degradation*, I mean your organization’s ability to identify the event and its consequences, and establish minimal stable functionality, *i.e.*, to “devolve” the organization to the most robust, less functional configuration available in the least disruptive manner possible, and to begin to direct initial efforts for rapid restoration of services in a timely fashion. The integrated approach embraces the blending of strategy, competitive intelligence, event management, and consequence management as key driving forces for business continuity.

Businesses (and governmental entities) are complex systems operating within multiple networks. These systems are composed of people, knowledge (often referred to as information and intelligence), strategy, competitive intelligence initiatives, event management capabilities (or lack thereof), relationships and inter-relationships, spheres of influence, equipment, and facilities. Simply put, these are physical and non-physical elements.

[Chapter One]

ENTERING THE AGE OF UNCERTAINTY: WHAT TO EXPECT

Chapter Summary

This introductory chapter provides an overview of the potential situations businesses may face in this time of uncertainty. In this chapter, we will begin our investigation into the development of an effective and, as may be possible, comprehensive business continuity process. We will also discuss the basis for developing vertically and horizontally integrated business continuity systems.

This chapter is designed to provide the reader with sufficient background material to allow you to focus your efforts when developing your organization's "integrated" business continuity process. This and the subsequent chapters in this book build on my two previous books. The first book, entitled *It Can't Happen Here: All Hazards Crisis Management Planning*, published by PennWell in 1993, provides the conceptual background for an approach to the development of an effective "all hazards" event man-

Introduction

Before we can discuss in detail the elements of the “integrated” business continuity process, it’s useful to summarize the basic assumptions on which this book has been written. These basic assumptions serve to form the foundation for the framework of the “integrated” business continuity process and this redefinition of business continuity.

Assumption 1: Businesses are Complex Systems Operating within Multiple Networks

As depicted in Figure 1-1, modern businesses are complex systems with many touchpoints. Complex business systems, however, generally can be grouped into five essential elements of analysis (EEA):

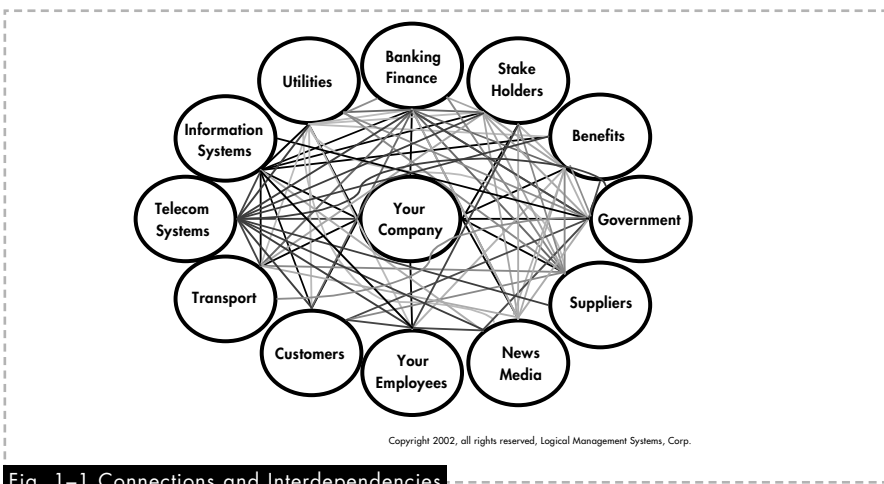


Fig. 1-1 Connections and Interdependencies

- Human resources
- Equipment resources
- Information resources
- Facilities resources
- Operational resources

Executive Order 13224 signed by President Bush on Sept. 23, 2001 blocks the assets of organizations and individuals linked to terrorism. According to a summary printed in *Counterterrorism & Security Reports*, vol. 9, no. 5, 168, such groups, entities, and individuals are covered by the Executive Order. A complete summary of the executive order (Executive Order 13224 - Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support Terrorism) can be found at www.ustreas.gov/terrorism.

While a complete listing of the organizations covered by the Executive Order is beyond the scope of this book, you can go to www.state.gov/s/ct/rls/fs/2001/6531.htm and find a complete listing.

Executive Order 13224 is important, both because of what it identifies and says, and because of what it does *not* identify and/or say.

While Executive Order 13224 lists some 168 groups, entities, and individuals, it does not list any domestic (U.S.) groups, entities, or individuals bent on committing terrorist acts. I found an interesting website as I researched this: www.tolerance.org provides a map of the U.S. depicting 676 “hate groups” not covered under this Executive Order. One only has to look at the anthrax events and wonder, why not?

In the U.S. and throughout the world, critical infrastructures upon which we all depend for the quality of life we enjoy are at risk. While business leaders express their concerns and list their most compelling topics (Table 2-2), the further away from September 11th that we get without another event, the more relaxed we may become.

Concluding Thoughts

Identification and protection of critical infrastructures will become increasingly important to organizations as they develop their business continuity strategy. Business continuity planning, in the traditional sense, is outdated before it can be implemented. In the next chapter, I offer a suggestion for a new definition of business continuity. However, in closing this chapter, we cannot overlook the importance of the infrastructures that an organization depends on for its existence.

The U.S. is in the midst of a tremendous cultural change—a change that affects every aspect of our lives. The accelerating reliance of our infrastructures on information systems and the cyber dimension is blurring traditional boundaries and jurisdictions. Critical infrastructures are central to any organization’s survival. We must lay the foundations for identifying our infrastructure touchpoints and understanding our infrastructure dependencies as we shape business continuity thought.

and generally lack any capability to analyze either business implications or public sector actions resulting from an event. This can be costly for an organization in today's business environment.

Building a comprehensive planning system is not difficult. In my book entitled *It Can't Happen Here: All Hazards Crisis Management Planning* (PennWell), I focused on developing a planning system based on an application of the incident command principles to the business setting. This still holds true today. Figure 3-5 summarizes the functions generally associated with an integrated event management system.

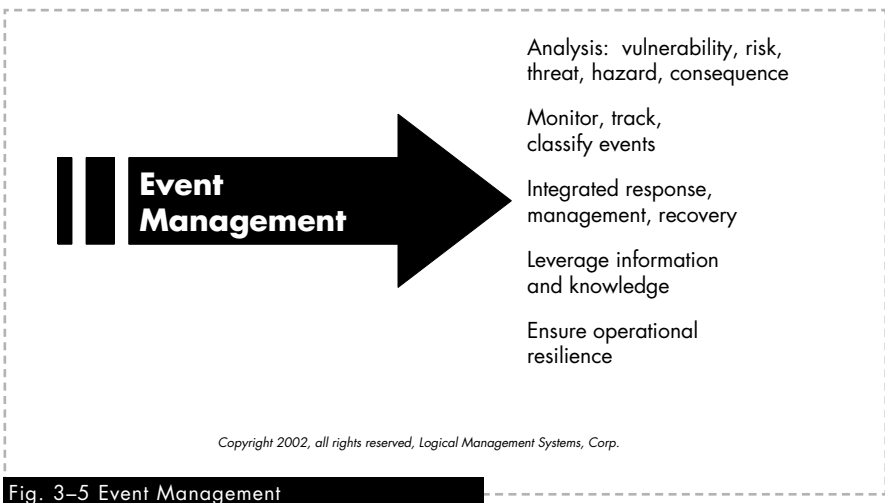


Fig. 3-5 Event Management

Business decision-making and decision-application can be broken down into eight elements. The enhanced incident command system successfully adopted by many client organizations also can be subdivided into eight parts. This may sound like an over-simplification of a complex process. However, please bear with me as I offer Table 3-1 as a simplified explanation.

Introduction

We are all conscious of time in today's business world. Everything from "just-in-time" delivery, to production and distribution, to the speed of information processing is based on time. Business continuity, as defined, is also based on time. Time is a factor. "Time will tell" if your organization grows, prospers, survives, and is resilient to disruptive events. When developing the concept of business continuity thinking, time was a critical factor.

I am going to introduce concepts, addressing how one can determine what is "time-critical" to the organization. The definition may vary slightly from organization to organization. However, for our purposes, we will define time-critical as:

The loss of any business function, related value-chain component, internal and/or external infrastructures, such that the result of that loss poses an imminent threat to the survival of the enterprise.

In the chapter overview, I provided a list of potential time-critical issues. Figure 4-1 depicts some of the potential events that organizations face today. We will discuss each and provide examples of analysis tools you can use to determine how these may be time-critical to your organization.



Fig. 4-1 Where's Your Next Event Coming From?

Time-Critical Issues for Analysis	What makes this a time-critical issue?
Loss of critical infrastructures	
Telecommunications/information systems	
Transportation (air, land, water)	
Disruption of emergency services	
Utilities (gas, electric, water)	
Energy supply	
Critical services	
Access denial	
Degradation/loss of critical operations	
Loss/degradation of operational capability	
Loss of electrical supply sources	
Loss of telecommunications/information sources	
Loss/degradation of buildings/occupancy	
Disruption of transportation	
Disruption of water supply	

Table 4-11 Thinking Through Development of Time-Critical Elements

Concluding Thoughts

When looking at time-critical events, you need to take into account strategy, competitive intelligence initiatives, and event management as they relate to how your organization will address these issues.

We have included examples of how best to assess time-critical events and some that your organization may wish to consider as starting points for assessment and analysis.

As with previous chapters, this is intended to build upon your assessment capabilities. You should be able to apply these concepts to develop a listing of time-critical events that would have potential impacts at all levels within your organization and its value chain.