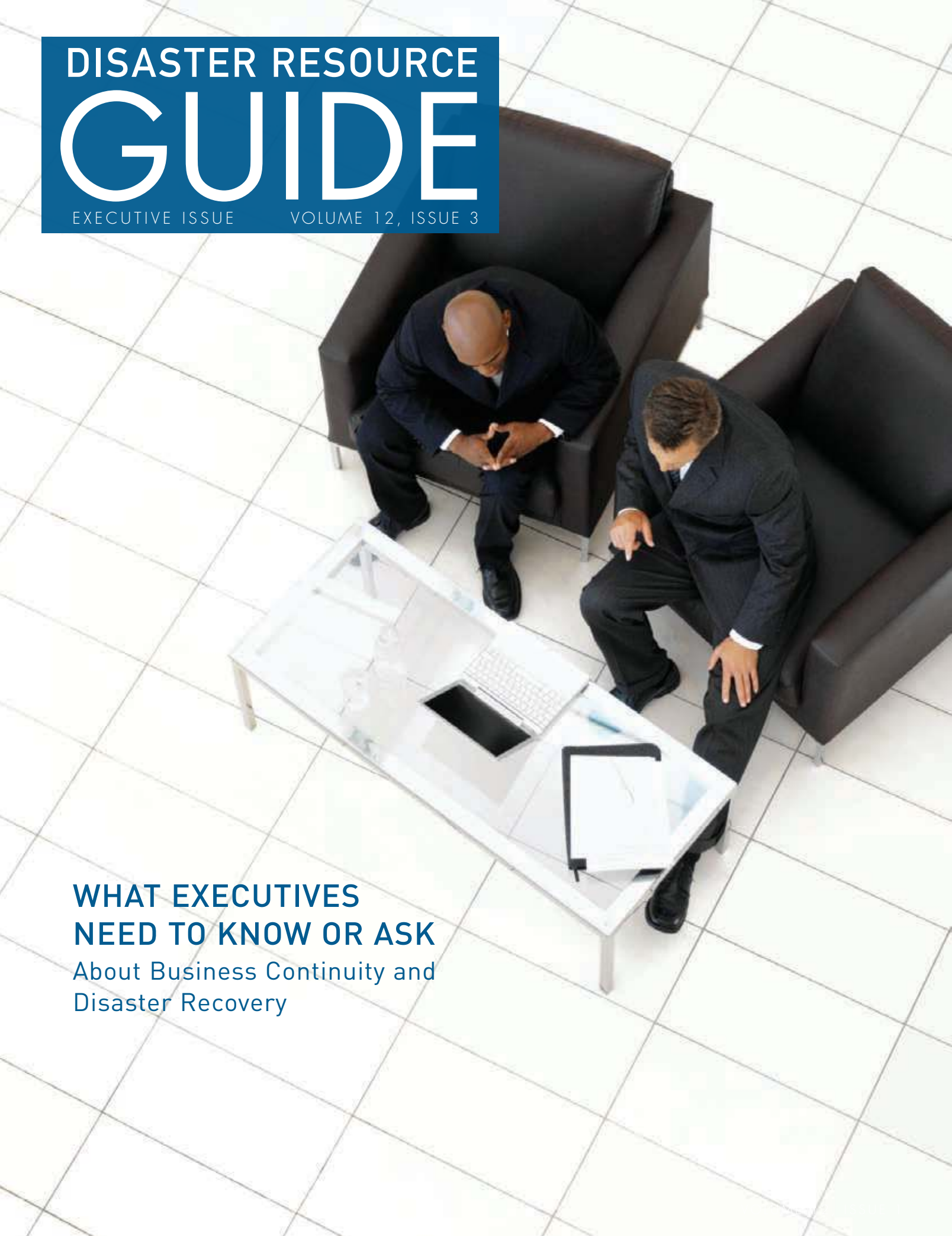
DISASTER RESOURCE GUIDE

EXECUTIVE ISSUE VOLUME 12, ISSUE 3



WHAT EXECUTIVES NEED TO KNOW OR ASK

About Business Continuity and Disaster Recovery

STROHL SYSTEMS

PLAN. PRACTICE. PREVAIL.

Business Continuity Leadership

A matter of experience and design – not chance

When you're talking about the survival of your business, a critical planning edge becomes a necessity, not an option.

There is no substitute for the proven expertise and insight of Strohl Consulting Services - a team of certified professionals who are highly experienced in all aspects of business continuity program management, including impact analysis, risk management, planning, testing and maturity assessments.

For more information on our entire set of services, please contact us at 800 634-2016, +1 610 768-4120 or info@strohlsystems.com.

Strohl Systems delivers the expertise and resources to help you build plans, practice for disruptions and prevail over disasters. Our formula is simple -

Plan. Practice. Prevail.

If you're ready to build plans the proven way, visit us online at www.strohlsystems.com.

FROM THE PUBLISHER

This morning I spoke with the folks at Standard & Poor's about their proposal to include a company's Enterprise Risk Management (ERM) function as a part of S & P's ratings of public companies. While the final decision about this risk evaluation and how it will be incorporated into ratings isn't expected for several weeks, this is certain to get the attention of the C-suite. "The times they are a-changin!"

Business Continuity Planning (BCP) evolved from the IT function of disaster recovery, which was all about backing up mainframe computers on tapes and having the capacity to restore the IT functionality quickly. In many organizations, BCP still sits, often buried, in the IT department. Read the article on BCP and ERM beginning on page 6, by John Phelps. On a related note, Robert Giffin shares more about the value of BCP on page 18.

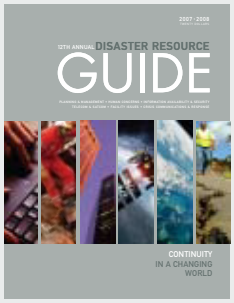
Our interview with Al Berman, co-chair of a Sloan Foundation committee addressing corporate preparedness, can bring you up to speed on evolving standards and regulations. In addition, Rebecca Levesque describes three recovery exposures many companies are not addressing today. And what if something does happen to your company…a toxic spill, workplace violence, the avian flu? Bruce Blythe is an expert on crisis communications and provides 5 principles to guide you. Damian Walch discusses your supply chain risks, and John Jackson highlights the importance of interdependencies and how they affect your BC planning.

As a part of our ongoing effort to raise the visibility of BCP, the Disaster Resource GUIDE is in the midst of a study on where BCP should report within an organization. Let us know if you'd like to contribute. And if you want a copy of this new study, please sign up for the e-GUIDE (see right). To read the study won't cost you a dime. On the other hand, to ignore this issue…

Tommy Rainey
Publisher

publisher@disaster-resource.com

ANNUALLY



The DISASTER RESOURCE GUIDE

Since 1996, the annual GUIDE has brought together the best of the best in one single volume. To subscribe, visit www.disaster-resource.com/freeguide

QUARTERLY

Mini-GUIDE

Each of the 3 new quarterly issues delves deeper into a single content category (i.e. Facility Issues, Telecom/Satellite, Education, Technology, etc.)

WEEKLY

The Continuity e-GUIDE

Every Wednesday the e-GUIDE provides a concise seven-day snapshot of the business continuity and emergency management industry from around the world. Visit www.disaster-resource.com/freeguide.

24/7

The Online GUIDE

Connecting via searchable products, services, and news archives, including recent news and press releases, the website provides a concise, accessible, updated resource. www.disaster-resource.com

QUARTERLY DISASTER RESOURCE

GUIDE

VOLUME 12 • ISSUE 3

On the Web Visit the Online GUIDE for more on this subject. **www.disaster-resource.com**
• Crisis & Emergency Management • Disaster Recoverey • Business Continuity • Homeland Security

THE ESSENTIAL PANDEMIC KIT

INCLUDES:

Forrester report on avian flu response, white paper on pandemic communications, and more.

DOWNLOAD YOUR FREE RESOURCE KIT TODAY!

www.varolii.com/pandemickit

VAROLii CORPORATION™

BUSINESS CONTINUITY PLANNING
AND ENTERPRISE RISK MANAGEMENT

BY JOHN R. PHELPS

Disasters like 9/11 and Hurricane Katrina have arguably changed the "worst case scenario" paradigm for business continuity planning and risk management. Shortly after Katrina struck New Orleans, many business continuity planners were hauled into the C-suite to explain how such a tragedy would have impacted their company. In many cases, the person responsible for Business Continuity Management (BCM) was instructed to draft a plan to address a "Katrina-like" event.

Many of us with both a BCM and Enterprise Risk Management (ERM) responsibility felt somewhat conflicted because, although it is important to have a plan for such an unlikely catastrophe, there are other serious risks that have a nearly certain likelihood of occurring. Risks like privacy, fraud and inaccurate data cost many organizations millions of dollars each year. Emotions run high in the face of rare and disastrous events, causing a rush to allocate funds and efforts to safeguard against them. Integrating BCM as part of a comprehensive ERM program allows a more reasoned and less emotional understanding of the universe of business risks faced by the company. This approach produces efficiencies with regards to how organizations react to catastrophic risk.

ERM provides the context with which to understand risks and how they interact with the business enterprise. By including BCM into such a program, the organization begins to understand how BC planning fits with other risks like the colors of a rainbow. In order to understand how both highly skilled fields can compliment each other, it is important to understand what ERM means.

What Is ERM?

Most people associate "traditional risk management" with the guy that buys the insurance. For years, risk management professionals were relegated to paperwork and number crunching behind closed doors. For the past twenty years, risk management focused on

dealing with insurable risks, as opposed to operational risks where outcomes can be influenced by how the risks are proactively managed. In other words, risk managers never felt they had a role in helping the organization to manage market, reputation or outsourcing risks. Instead, their expertise was applied to property, liability, and worker injury risks. In this context, business continuity and risk management were content to coexist in very separate "silos" of responsibility, failing to take advantage of the efficiencies offered by integrated risk assessment and treatment.

Within the past several years, the term Enterprise Risk Management was coined to distinguish traditional risk management from a more comprehensive and pro-active view of operational risk in an organization. ERM is a business capability and requires the organization to look at risk from a completely different perspective – as a partner and source of opportunity for the business. The question is, how can the enterprise risk manager help operational areas take those risks and use them to the advantage of their companies. In order to take risks intelligently, the organization needs a construct to evaluate risks from the boardroom to the mailroom – from power outages to hurricanes to data management or threats to brand equity.

The other distinguishing aspect of ERM is that the risk management department does not own the process. Done correctly, ERM will be embedded into the operational areas and systems. The risk manager may be the wizard of tools and steward of the governance structure, but application of the process is "owned" by the business units. In a mature structure, leaders and managers in areas like brand, finance, human resources, facilities and information technology understand their risk management responsibilities. There is a common governance structure that brings these disciplines together to provide oversight of the process and how it is pro-actively addressing risks like reputation, data quality, privacy of information and, yes, business interruption.

BCM and ERM, Together At Last

BCM and disaster recovery are natural components of ERM. All the resources and plans that make up a business continuity plan are developed to address business interruption risk in an organization and should be part of a comprehensive mitigation plan for all the enterprise risks.

For the last few decades, the analysis of business functions has been based upon an "impact" perspective as developed during a business impact analysis (BIA), the gold standard used to determine "criticality" of business functions. The purpose of a BIA is to assess the impact a business function has on the overall organization and to develop recovery objectives. It is not designed to provide a full risk assessment. In other words, the BIA does a poor job of assessing the likelihood of disruption to business functions and the effectiveness of controls already in place. In addition, it rarely, if ever, evaluates the business continuity risk against a tapestry of other enterprise level risks.

More mature ERM programs have the force of corporate policy that requires leaders and managers to understand risk before they take it. At Blue Cross and Blue Shield of Florida, the process starts with the BIA and is then run through the Enterprise Risk Management filter, to add the "likelihood" and "effectiveness of control" perspective. A key component of the process is the tools that have been created for the ERM program, especially the method and evaluative criteria for assessing risk. This provides a unified understanding of each risk based upon the same criteria. This method is used for all risks, including business interruption. The outcome of the ERM assessment process is the development of a specific risk index. Two different functional areas with the same impact may have very different risk indices when calculated using the ERM methodology. This helps management understand two important dimensions. First, by comparing the risk indices, a greater understanding is created of which "important" functional areas are more important than others. Second, management can understand how the risks of interrupting important business functions compare to other risks in the company like reputation or market risk. This supports decisions concerning the allocation of limited resources in terms of risk treatments. Specific to business continuity, in some cases, this process causes the organization to re-consider the application of planning resources for certain functional areas. This perspective would not have been known had management relied upon the BIA alone.

ERM, by its definition, is a very high-level view of risk in an organization. A component part of an ERM program is the mitigation of catastrophic risk from natural and human causes. Many organizations are beginning to recognize the opportunity they have from embedding or incorporating BCM into an overall program to identify, evaluate and mitigate risk. Boards expect the organization to have a comprehensive and effective process for identifying, measuring and managing risk. By viewing BCM as a risk management function and embedding it into the enterprise level ERM program, which has been aligned with the strategic imperatives of the company, boardroom expectations are met and alignment achieved.

The term was coined to distinguish traditional risk management from a more comprehensive and pro-active view.

Joining ERM And BCM

Both BCM and ERM use scenario analysis to drive planning. After being approached to develop plans for Blue Cross and Blue Shield of Florida in the event of another Hurricane Katrina, the hurricane threat was modeled using an outside catastrophe modeling company. Modeling revealed that the odds of the home office being struck by a Category-3 hurricane or higher, are once every 70,000 years. In addition, each of the buildings were designed to withstand category 3 hurricanes, and the new, state of the art, hardened data center is located 20 – 30 miles inland from the home office facility. This caused management

CONTINUED ON PAGE 8

CONTINUED FROM PAGE 7

to think differently about the resources it would take to relocate thousands of critical employees for a "smoking hole" type event. As a result, a staged approach was chosen to emphasize more likely scenarios but provide some pre-planning in case the worst-case scenario does happen. The hurricane scenario analysis gave us another prism with which to view our hurricane risk.

Scenario analysis can be effectively used for a multitude of risks other than hurricanes, pandemics or power outages. The process is equally valuable for events like unintentional release of data, unethical boardroom shenanigans, and supply chain failure. To illustrate how BCM and ERM can work together, consider a regulated company that needs to make state filings for rate increases. During the BIA, it was reported that the risk of lost revenue from not making timely filings (as a result of a major, unexpected disruption like a fire or long term power outage for example) would be in the range of $2 – $5 million per week. Through the BIA lens, then, this department would be deemed critical.

After the BIA, the people in the department responsible for the filings were interviewed using an ERM process of risk profiling. The risk of not making the filing (interruption of services from the filings department) was evaluated according to impact (similar to BIA but with an established ERM scale and criterion), likelihood and effectiveness of controls. These factors were combined into a single risk index for that specific department. It was determined that the risk index was relatively low due to existing controls including the ability to re-file renewal increases post disaster. This perspective indicates that the filings department is not "critical" after all. In other areas, the Enterprise Risk Management Assessment supported the BIA findings. For example, customer service functions were critical under both the BIA and the ERM assessment. What this supports is a decision around the application of limited resources. Developing extensive plans to recover customer service areas within a minimal amount for downtime is essential. Allocating resources to recover the filings department is foolish. Ah, the efficiency of ERM!

Three Models for ERM and BCM in a Company

When joining together BCM and ERM, there are three different models. The first model is having a central management for both BCM and ERM, which is Blue Cross and Blue Shield of Florida's model. The second model is to create a shared responsibility with BCM and integrate it functionally into the ERM program. The third, and least efficient way to maintain BCM and ERM programs, is to maintain separate silos for both disciplines. Unfortunately, this is what many businesses are doing today. The danger of maintaining separate BCM and ERM efforts – the "silo mentality," is that both are working according to their own strategy. Nothing could be less efficient or effective.

To support the integration of ERM and BCM, Blue Cross and Blue Shield of Florida has created a risk council to provide a single governance structure. The risk council is made up of director level representatives from Information Technology, Human Resources, Service, Compliance, Internal Audit and so forth. The risk council is responsible for "controllership" of operational risk as well as general oversight and control. Part of the oversight responsibility extends to BCM and provides assurance that understanding the business interruption risk and mitigation of that risk, is clearly understood and pro-actively addressed. High-level executive support has been established though the Operating Committee, which includes the Office of the Chief Operating Officer.

The Katrina Effect

When we consider large, highly publicized risks similar to Hurricane Katrina, management often reacts emotionally. "What would we do if it hit OUR company? How would we serve our customers? This could bankrupt the company!", and so on. These are serious questions, but while management panics about such improbable occurrences, companies could bleed millions of dollars per day from other risks like fraud and "dirty data". Organizations need to address the "Katrina-like" event, certainly, but they need to do so as part of a comprehensive understanding of all the company's significant business risks.

ERM helps provide an understanding of the relationship of risks, which cannot be obtained from a traditional risk management or business continuity perspective. ERM and its associated methodology and tools provide an opportunity for business continuity professionals to burst out of their silo to observe how business interruption risk relates to the other enterprise level risks. This approach also elevates BCM to a higher level with Boardroom and c-suite attention. Companies that can achieve this level of maturity with their business continuity program will make better decisions about the allocation of limited capital.

There are few organizations that have taken their business continuity program to this level. The psychology of risk is one that constantly gets in the way of making truly informed decisions. Without factual and logical risk assessment methodologies, emotion at all levels of the organization will triumph reason. Throughout the world, in every organization, people are making decisions about risks based on past experiences and emotions. ERM and its methodology will continue to fly the banner of reason in a battleground of emotion. At one time, people relied on the woolly caterpillar to tell them about how harsh the winter will be. Now we have meteorology. In just the same way, an ERM approach to understanding business risk will help the BC professional declare victory over the business interruption risk. The woolly caterpillar of business continuity is about to become extinct.

ABOUT THE AUTHOR

John R. Phelps, CPCU, ARM, CBCP is Director, Business Risk Solutions for Blue Cross and Blue Shield of Florida, Inc. Mr. Phelps is responsible for the development and implementation of an Enterprise Risk Management program for the company, and is a leading practitioner of ERM. Prior experience includes nearly two decades managing risk systems within the healthcare industry.

Distinguish yourself in Business Continuity through professional certification from DRI International.
Position yourself as a recognized leader in the field worldwide with a basic, experienced or advanced certification.

The Best Instruction in the Field of Business Continuity Planning

Our review courses are packed with interactive instruction, case study analysis, problem-solving methods, and thorough coverage of the ten Professional Practices for Business Continuity Professionals. Every instructor is a certified professional with superior knowledge of and an average 20+ years experience in the field of business continuity. Our courses are the first step to validating your expertise, highlighting your professional skills, demonstrating your commitment and increasing your professional value as a professional Business Continuity planner. **Register today**.

Get started immediately with the ease of visiting our website. You will find courses conveniently located in a dozens of cities. Or, for added convenience choose an online course and a Qualifying Exam available through a local Prometric testing center near you.

DRI
the institute for continuity management

+1.202.962.3979

www.drii.org

STRATEGIC CRISIS LEADERSHIP:
BEING AN EFFECTIVE LEADER IN THE MIDST OF CHAOS

BY BRUCE T. BLYTHE

What would you do in the following three situations?

Crisis Leadership Moment #1

Imagine that it finally hit! The avian flu has just been confirmed to be contagious. One of your traveling employees has just been diagnosed with this dreaded disease after returning home. Your workforce is fearful that they might have been exposed and most are not personally prepared at home for an outbreak. But, you need them to carry out the company's business continuity plan. Employees in mass want to take time off. What do you do?

Crisis Leadership Moment #2

You learn that one of your facilities has been emitting low-level toxic substances for an undetermined amount of time. It is the company's fault due to a prior decision to delay replacement of a faulty system in one of your facilities. But, it is quickly remedied. Possibly, employees, visitors and others have all been exposed to a small degree. Most likely, the exposure was minimal with no harm.

Unfortunately, a similar situation occurred at the same facility last year. You reported it to the authorities and the media, in learning about it, exagerated the story, blaming the company for putting people at risk.

If knowledge of the present toxic emission were unveiled publicly it would likely cause serious reputational and legal damage to your organization, now that it has happened again. But it would be worse if discovered later that you tried to cover it up. Possibly, your position within the company is on the line, as well. Only you and a couple of trusted subordinates know about the emission now. Do you proactively go public and risk the feared personal, reputational and legal damage or try to resolve the situation quietly with (hopefully) no public harm done?

Crisis Leadership Moment #3

Two bombs hit your facilities simultaneously in different locations with a note from an activist group taking credit. Do you close all your facilities throughout the enterprise as a safety precaution? If so, for how long? If not, what are alternative responses?

Preparedness

Each of these situations requires a "defining decision." Initial information is usually wrong. Rumors are rampant. Action must be taken without time for sufficient consideration. The consequences are high. People are watching your every move. The velocity of information coming in is staggering. The stress is numbing.

Now, make those decisions that may have life and death implications. Act in a manner that will be scrutinized later. Take that risk that may define your career as an excellent leader when the organization needed it most...or an inept manager with poor judgment under pressure.

Crisis Leadership

There are significant differences between Tactical Crisis Management and Strategic Crisis Leadership. The table below gives some of the high level differences:

Tactical Crisis Management	Strategic Crisis Leadership
React	Anticipate
Short-term	Long-term
Process	Principles
Narrow focus	Wide focus
Tactical (implement)	Strategic (judgment)

Strategic Crisis Leadership involves high-leverage skills that are vital to corporate recovery in the midst of a disaster. Crisis leadership skills are needed that define the crisis beyond the obvious, forecast the intended and unintended consequences of decisions, anticipate the effects of the crisis on impacted stakeholders, assess the impact of the crisis on core assets, and follow the values and guiding principles of the organization – and, your own ethical standards that may be tested to the limit.

Crisis leadership is more about who you are than what you know. No learned crisis leadership skill will overcome a lack of character, ethics or integrity. An effective crisis leader must act deliberately, quickly, and effectively with honesty, high moral values and ethical standards.

In order to help assure their leaders will act with good character in a caring manner when crises hit, crisis prepared organizations develop overarching response guidelines for their crisis managers to follow. I provide you with five guiding principles for managing crises:

> "No learned crisis leadership skill will overcome a lack of character, ethics or integrity."

1. Well-being of people first, with caring and compassion
2. Assume appropriate responsibility
3. Address needs of all stakeholders in a timely manner
4. All decisions and actions based on honesty and ethical guidelines
5. Available, visible and open communication with all impacted parties

Be, Know, Do

The U.S. Army defines the three basic components of leadership as Be, Know, Do. "Be" is about who you are. "Know" is about the skills and knowledge you have acquired. And "Do" is about the actions that you take on a timely basis. Purposeful attention to all three components of Strategic Crisis Leadership will increase the likelihood that you'll know what to ask, what to do and how to do it. And more importantly, learn to manage the unexpected.

Be, know, do...what are the skills needed to meet these Strategic Crisis Leadership responsibilities? There are many. But here is a simple introductory prescription for effective crisis leadership.

What do you need to be? Caring. Demonstration of caring is more important than all other leadership traits combined, according to research by the Center for Risk Communications. If you come across as uncaring, people will become outraged. Caring during crisis response is not a feeling. Caring is a set of corporate and personal behaviors that elicit the perception in impacted stakeholders that you and your company truly care.

What do you need to know? As a leader, you must have a vision for crisis resolution. Without a clear and compelling vision for response and recovery, you will not be able to adequately lead your people during times of crisis.

And do? The single most important action is two-way communication. Simply put, you will never be any better at responding to crises than your communication. That involves how well you listen to obtain the facts, and how well you speak openly to impacted stakeholders.

Scenarios Revisited

So, how does this apply to real life situations? I introduced three scenarios at the beginning of this article of dealing with avian flu, people exposed to a toxic substance, and the simultaneous bombing of two facilities by an activist group.

In applying effective crisis leadership principles, I recommend that you look at three rules of thumb to focus your response. First, identify the core assets of the organization that are potentially at risk. Are people in harm's way? Is there possible damage to your company brand, reputation or shareholder value? Will the ability to deliver goods or services be significantly disrupted? Secondly, identify all stakeholder individuals and groups who are harmed (real or perceived). Do your best to address their needs and concerns. And third, anticipate the potential progression of events and reactions by stakeholders.

With the avian flu scenario, consider first addressing the well being of your most important asset, your people. Provide masks, gloves, and hygiene protocol within the workplace. Get your hands on cash, food and water. If you don't

CONTINUED ON PAGE 12

CONTINUED FROM PAGE 11

already have these things, move fast. The early bird gets the worm during crisis management. Once your people are addressed, focus on stakeholders who might need priority attention. It could be customers, or your suppliers and distributors. Prioritize and do what you can to address the needs or concerns of all impacted stakeholders. Those stakeholders that you don't adequately address will likely be the problem areas. Anticipate their needs by imagining what you would want or expect if you were in their position.

The toxic exposure scenario involves information that is known to you, but not to those who may be at risk. It would be easy for uninvolved advisors to recommend that you come forward immediately and let the chips fall where they may. It's hard to hide damaging information and is best to follow the guiding principles of taking responsibility in an honest and ethical manner. In general, good crisis management will require protection of the greater good over personal concerns. With that said, there are times in the real world of crisis management when the decision is made to conceal known information. Right or wrong, if the damage of being forthcoming is considered too much to bear, some people will decide not to come forward. If you are tempted to conceal, you must come up with a rationale that will pass the "reasonable person test." Consider confidentially getting a multidisciplinary group of advisors to discuss your best alternatives. Possibly, a specialist in toxic exposure should be consulted. Anticipate the reactions of people who perceive harm if they learn of your concealment. If you do not feel comfortable defending your rationale on the front page of the newspaper, you are taking a serious risk that could take you and or the company down. Lying and concealing information are two ways to escalate the severity of your crisis. Think: Arthur Andersen, Bill Clinton, and Martha Stewart.

Finally, the scenario of a simultaneous bombing in two work locations was presented. Your employees and customers (if they come onsite) will have the natural fear of reoccurrence. The issue emerges of not wanting to reinforce the violent acts of a hostile activist group. Shareholders may have fears that their investments are not secure. The media may sensationalize the story and even look for ways to blame your company. Your job of crisis leadership is to anticipate these and other reactions by impacted stakeholders and address their needs. A strong physical security response may be needed to help assure employees and customers. Possibly, an aggressive approach to help apprehend the offenders would be effective, like offering a generous reward for information and arrest. Methods for efficiently giving and receiving communications would be a vital component for dealing with this crisis.

Summary

With no prior notice, you must make on-the-spot decisions and implement rapid-fire responses when crises unexpectedly strike. Your people will be stressed-out and deadlines time-compressed. Information will be inadequate and the high-consequences of your responses could determine if people will be harmed, careers ruined and your company seriously damaged.

Experience and empirical research all seem to agree. It is best to prepare. Crisis leadership planning, training, tabletop exercises and simulations – they all play an important part in helping you become a crisis leader. Hopefully, these guidelines will help you begin the important journey toward personal and organizational crisis preparedness.

ABOUT THE AUTHOR

Bruce T. Blythe is the CEO of Crisis Management International, a worldwide consulting firm that provides corporate crisis preparedness and response services, including Business Continuity, Disaster Recovery, Emergency Response, Crisis Management, Human Impact Response, Threat of Violence Consulting, Workplace Violence Programs, and Strategic Crisis Leadership development. You may contact the author at (404) 841-3402 or bblythe@cmiatl.com.

Wallace Information Communicator

Mobile Emergency Management for the Enterprise

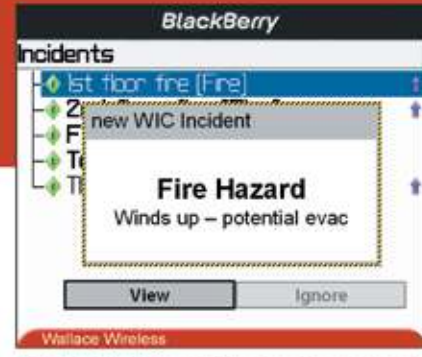
Safeguard your organization against any emergency or disruption to business by ensuring critical information is mobile, always up-to-date and you can dependably communicate within the entire enterprise.
WIC combines all of this in a single solution, for all your notification needs.

Image: NASA/MODIS Rapid Response

Up to date accurate information wherever, whenever.

WIC provides...

- guaranteed access to emergency contacts in a crisis
- information required to make decisions, stored on the device
- remote data capture - mobile workers can immediately upload data from the field
- the ability to monitor and manage the crisis response team



Dependable crisis management at your fingertips

Wallace Wireless

crisis management beyond email

wallacewireless.com

EVOLVING STANDARDS AND REGULATIONS – THE NEW BUSINESS CONTINUITY LANDSCAPE

AN INTERVIEW WITH ALAN BERMAN, CBCP, MBCI

The Disaster Resource GUIDE recently interviewed Mr. Alan Berman, a noted author and worldwide speaker on the subject of business continuity regulations.

Mr. Berman is a CBCP, MBCI, and NFPA committee member, a member of the NY City Partnership for Security and Risk Management, Treasurer and Executive Director for Disaster Recovery Institute and the co-chair for the Alfred P. Sloan Foundation committee to create the new standard for the US Private Sector Preparedness Act (PL 110-53). Over a career that has spanned 25 years, he has served as a President and CIO for a major financial institution, National Practice Leader for Operational Resiliency for PricewaterhouseCoopers and Global Business Continuity practice leader for Marsh.

Disaster Resource GUIDE: There seems to be a lot of activity centered around Business Continuity regulations, guidances and standards these days. Any comments?

Mr. Berman: The combination of a British Standards Institute (BSI) standard and a US requirement to create a private sector preparedness standard (Title IX of the US Private Sector Preparedness Act) arriving within a short span of each other has created a flurry of activity around regulations and standards. In reality there has been increasing activity over the last 25 years, especially since 2001. The chart below provides some indication as to the volume and frequency of regulatory, standards and guidance activity.

Q: Can you define the use of regulations, guidances and standards?

A: A regulation is created and enforced by a recognized regulatory body; e.g., the Securities and Exchange Commission, the Federal Reserve or a federal, state or municipal authority. Regulations tend to be mandatory and punitive. Guidances are produced by professional organizations that provide "best practices" for various operational and control matters. Standards, for the sake of this discussion, are formally approved policies, procedures or instructions from a recognized standards body, for example the American National Standards Association (ANSI) or the International Standards Association (ISO). Standards like guidances are non-punitive, but carry the positive connotation of providing a "seal of approval" for organizations that can perform up to the standard.

Q: But aren't most regulations and guidances centered on the financial industry?

A: Certainly, the financial sector (banking and investment firms) has been at the forefront of the regulations and has invested the most money in creating a more resilient processing and information model. In the US the FFIEC (Federal Financial Institution Examination Council), which governs the operations of federally chartered banks, has been around the longest, and in my opinion is the most robust of all the regulations. It is used by both state and federal bank auditors and provides the most comprehensive set of detailed implementation and review procedures. The SEC, NASD and NYSE have created

BC STANDARDS AND REGULATIONS: PRIOR TO AND POST 9/11

1991 – 2001

- Consumer Credit Protection Act
- OMB Circular A-130
- FEMA Guidance Document
- Paperwork Reduction Act
- FFIEC BCP Handbook
- Computer Security Act
- 12 CFR Part 18
- Presidential Decision Directive 67
- FDA Guidance on Computerized Systems used in Clinical Trials
- ANSI/NFPA Standard 1600
- Turnbull Report (UK)
- ANAO Best Practice Guide (Australia)
- SEC Rule 17 a-4
- FEMA FPC 65
- CAR

2002 – 2008

- Sarbanes-Oxley Act of 2002
- HIPAA, Final Security Rule
- FFIEC BCP Handbook
- Fair Credit Reporting Act
- NASD Rule 3510
- NERC Security Guidelines
- FERC Security Standards
- NAIC Standard on BCP
- NIST Contingency Planning Guide
- FRB-OCC-SEC Guidelines for Strengthening the Resilience of US Financial System
- NYSE Rule 446
- California SB 1386
- Australia Standards BCM Handbook
- GAO Potential Terrorist Attacks Guideline
- Federal and Legislative BC Requirements for IRS
- Basel Capital Accord
- MAS Proposed BCP Guidelines (Singapore)
- NFA Compliance Rule 2-38
- FSA Handbook (UK)
- BCI Standard, PAS 56 (UK)
- Civil Contingencies Bill (UK)
- FPC 65
- NYS Circular Letter 7
- ASIS
- State of NY FIRM White Paper on CP
- NISCC Good Practices (Telecomm)
- Australian Prudential Standard on BCM
- HB221
- HB292
- BS25999
- SS507
- TR19
- CA Z1600
- ISO/PAS 22399
- DRII
- Title IX – 110-53

their own standards and operational review procedures to govern security dealers. The financial standards can be seen around the world from the FSA (Financial Services Authority) in the UK to the MAS (Monetary Authority of Singapore) in Asia to the more global Basel Committee's Capital Accords and Sound Practices for the Management and Supervision of Operational Risk. In essence, the financial world has recognized the impact associated with any operational interruptions.

But it is also important to realize that there are business continuity regulations associated with other industry sectors. Energy has FERC (Federal Electric Reliability Council's Security Standards for Electric Market Participants) and NERC (North American Electric Reliability Council's Security Guidelines for the Electricity Sector). Health care has HIPAA (Health Insurance Portability and Accountability Act) covering all healthcare providers who transmit or store patient healthcare information, as well as JHACO (The Joint Commission on Accreditation of Healthcare Organizations), and the FDA (Federal Drug Administration) good practices for manufacturing, laboratory and clinical testing, as well as for computerized systems, just to name a few other industries.

In essence we are seeing more segments creating standards for business continuity.

Q: But aren't most of the activities centered on the recovery and/or continuity of the technology environment?

A: Fifteen years ago the answer probably would have been yes, but business continuity has become a more holistic process, encompassing all of the elements necessary to maintain the viability of the business entity during an interruption. Undoubtedly, the ability to use technology is a very important aspect of business continuity. But it is one of many vertical components of the entire operational environment. Consider the facilities, personnel, equipment, supplies, etc., all of which also play a key role in restoring operations to a state of normalcy. The regulatory bodies have also recognized this and have clearly pointed out that "Business continuity planning is about maintaining, resuming, and recovering the business, not just the recovery of the technology," (FFIEC 2003); "Business Continuity Management (BCM) is an over-arching framework that aims to minimize the impact to businesses due to operational disruptions. It not only addresses the restoration of information technology (IT) infrastructure, but also focuses on the rapid recovery and resumption of critical business functions for the fulfillment of business obligations," (MAS 2003); and "Business continuity management describes a whole of business approach to ensure critical business functions can be maintained or restored in a timely fashion," (Australian Prudential Standard – 2005).

The world has recognized the need to recover the business and operational entity as a whole, not just the technology components. In fact, given the recent concern over pandemics, which is clearly seen as a personnel issue having little to do with technology, it points out the need to take a holistic approach to business continuity.

CONTINUED ON PAGE 16

CONTINUED FROM PAGE 15

Q: What if my industry is not covered by a regulation?

A: Even if your industry segment is not specifically addressed by a regulation, companies may find that their customers will require that they adhere to the same regulations as the covered entity. For example, under appendix D of the FFIEC, "Institutions should review and understand service providers' BCPs and ensure critical services can be restored within acceptable timeframes based upon the needs of the institution. If possible the institution should consider participating in their provider's testing process." HIPAA provides for similar compliance from it's "business associates." So the burden on non-regulated organizations may even be more onerous than that of covered entities. A supplier may be forced by its banking clients to comply with the very strenuous FFIEC regulations, even if the activities they perform may be as minor as being a printer of forms used by banks.

And then there are the statutory considerations that may find companies and even governments negligent and subject to civil penalties for "failure to plan" or "failure to prepare." So it is very likely that in one way or another all entities are probably going to have to adopt a business continuity plan.

Q: What if I am a multi-national and have to comply with the regulations of many countries?

A: Very much like those entities that are being required to conform to customer regulations, multi-nationals will have to create a business continuity program that will have to allow them to adapt to regulations of the country in which they do business. That is why there is such activity around creating standards. The best business continuity programs provide "flexibility within a framework" to allow them to adjust some aspect of the plan to meet the requirements of varying jurisdictions.

This ability to adjust to varying rules is not dissimilar to adjusting to customer requirements. So having a good foundation for the planning process is critical.

Q: There are many people who are being pressured to comply with, but are not sure what to do. Any advice?

A: Wait – remember this is a VOLUNTARY standard. If you don't comply there is no penalty. BS25999 was announced with a lot of marketing fanfare provided by non-government training and consulting firms. The swirl of misinformation has created a sense of urgency, which does not really exist. Consider the fact that this is a British standard, not a global one. So if you rush out to meet this standard and the US one is different, you are likely to have done more harm than good.

Q: What about the US "Private Sector Preparedness Act"?

A: In August of 2007 the President signed into law PL 110-53. Title IX of that law provides for "Private Sector Preparedness." The law was originally intended to implement the recommendations of the 9/11 Commission. The essence of the recommendations from the commission was to implement the NFPA (National Fire Prevention Association) 1600 ANSI standard for the United States. Along the legislative route the words "or others" was added after NFPA 1600, opening up the possibility of considering other standards. This process is underway. DHS has appointed FEMA as the government organization responsible for creating the standard and overseeing certification of companies.

Q: I know you were involved in the effort to help create a standard that is being considered by the Department of Homeland Security, Federal Emergency Management Agency. Can you describe the effort?

A: I was fortunate enough to have been asked by the Alfred P. Sloan foundation to chair the committee to create the new standard. Working with some of the most dedicated people from the other professional organizations, we were able to draft what we feel is a workable and adaptable standard that will achieve the objective of making companies more prepared, without adding an undue burden on them. It provides for use of existing regulations and standards requirements that have eight basic elements needed to show preparedness. The idea was to provide credit for efforts already completed by many companies as part of their regulatory audit process and for those who have used existing recognized standards around which they have built their programs. This would include NFPA 1600, DRI International 10 professional practices, FFIEC, NERC, and other recognized standards. What we are trying to avoid is a reoccurrence of the expense and efforts that surrounded Sarbanes-Oxley compliance.

Q: Do you have any other concerns about the new regulations?

A: I am greatly concerned about the legislation's impact upon small and medium sized businesses that will bear an undue burden in an effort to comply. Although PL 100-53 has language with special considerations for small business, once the large companies decide to comply with the new standard, small and medium sized companies will be forced to comply in order to satisfy their customers' requirements. The government will be in no position to ask for relief for small and medium sized businesses, as the regulation is voluntary and hence not subject to legislative relief. The only practical way that small and medium sized companies can demonstrate their level of preparedness is for there to be tools available to them that will let them self assess their current state. A second set of tools can provide a means to help improve their preparedness. This will ensure their customers that they have attained a level of preparedness that will allow them to survive interruptions.

Q: Any final thoughts?

A: The use of recognized processes for creation of business continuity programs will serve any organization well. As the standard develops, it is very likely to embrace an established structured approach containing elements that are recognized by business continuity professionals. Those companies who have used such a process will find that they will have little trouble complying with the new standard.

According to Gartner, 4 out of 5 large enterprise corporations (80%) will fail to complete the successful recovery of all critical business applications and processes during their next test or incident on their first attempt.

21st Century Recovery Assurance Software Solutions

Be Exceptional!

21ST CENTURY software INC.

1-800-555-6845
www.21stcenturysoftware.com

PROTECTING YOUR BUSINESS FROM INTERRUPTION:
THE VALUE OF BUSINESS CONTINUITY MANAGEMENT

BY ROBERT GIFFIN, CBCP

The Need For Business Continuity Management

All businesses face the threat of an unplanned business interruption. While the causes vary from natural disasters to IT service interruptions, many organizations lack the capability to respond in an effective way. As a result, thousands of businesses large and small are crippled every year by unplanned business interruptions. However, there are cost effective protections that every business can establish to avoid this risk. Many of these protections are focused on isolated risks; for example, if a company has a critical product that has to be shipped no matter what – they may choose to store that product in two locations, thereby protecting it. However, such an approach ignores the broader purpose of risk management: to examine these risks in a structured approach will result in a comprehensive understanding of the organization's risks, thereby optimizing its investment to limit those risks.

The structured approach needed for business interruption risks is business continuity management – a process that analyzes an organization's risk of business interruption and takes actions to reduce it. While this is often achieved through a continuity plan, simply writing a plan will not substantially affect your business's exposure to interruption risks. A business continuity management process is the key to identifying which activities will reduce risk and eliminating the activities that are less beneficial. By taking a structured approach to managing business interruption risk, an organization maximizes its risk reduction while minimizing costs and focusing its efforts on critical areas that are worth protecting.

If it's not a plan, what's the outcome? Organizations that embark on

developing and implementing business continuity management processes often create well-rehearsed, documented business continuity plans. But they also create something more valuable: a well-aligned risk management culture that learns to proactively recognize business risk and take action, and when an issue persists, apply reactive frameworks to control the resulting impact.

The remainder of this article describes the business continuity management process and how each part of the process drives the effort towards value-added activities. Also offered is a simple, straightforward process to initiate business continuity management, and a number of key success factors.

The Process

Business continuity management is often daunting because of the number of ways it can be completed. With so many options, it's easy to get lost and tempting to just start doing things without an understanding of what you are trying to achieve. To better understand the basic building blocks of business continuity management and how each generates business value, here are the five key tasks that make up a solid business continuity management program and the strategic benefits they provide:

1. Identify critical activities and associated dependencies

This provides the analysis needed to focus the business continuity management process on the areas that will provide the most benefit. During the analysis, every area of the company should be evaluated to identify critical activities and dependencies that may not be immediately obvious. This typically includes an estimated cost of downtime and prioritization of when each activity would be recovered after a widespread disaster, thereby focusing business continuity management efforts on the shortest timeframes. The longer timeframes are not neglected, but they are activities that could likely be prepared for during an interruption due to the long lead time allowed.

2. Identify likely causes of failure and protections against failure

Some causes of failure are pervasive across every critical activity, such as natural disasters or power outages. Those causes can be protected with facility-wide plans to respond to the event and communicate the response to stakeholders. In addition to pervasive causes, each critical activity may have some unique causes of failure, such as equipment failure, loss of a specific technology or loss of key personnel. These unique causes may be controllable through redundancy or other protections like cross training. When the potential protections compare favorably to the estimated cost of downtime identified in task, a business case can be built for implementing the protection.

3. Develop alternate modes of operation for critical activities based on likely causes of failure

Critical activities that cannot be adequately protected from failure will need to have alternate modes of operation defined. For office personnel, this typically involves alternate work space or manual workarounds in the event of technology downtime. For more complex environments, this typically involves a process to redistribute work to other locations. It is likely that departments across the organization have theorized about how they would continue to work in the event of an interruption. These theories should be gathered, analyzed, documented and agreed to for critical activities. While some alternate modes of operation may have little increased cost (such as using unused office space for recovery), others will have significant cost (dedicated alternate office space for 200 employees). Each of the decisions made for alternate modes of operation should also be compared to the cost of downtime (identified in task 1) to determine the most cost effective option that matches management's tolerance for risk.

4. Document plans to implement the alternate modes of operation and manage the overall process of responding to a disaster and performing a recovery

Individual recovery plans will need to be developed to define the details of how each critical activity will deploy its set of alternate operating modes. In addition, executive level plans will need to be developed. These documents will identify the people responsible for making decisions, the resources needed and the methods of communication that will be used.

5. Exercise the plans

Even though it is the last step, exercising plans provides some of the greatest benefit to the organization. Exercising ensures that the personnel critical to the recovery effort are capable of implementing the company's plans. Exercising will also provide the most detailed and focused review of your strategies and plans.

The Result

Using the process above to analyze and evaluate the risk management options for an organization results in reliable and repeatable results. In addition, processes will result in the following key outcomes:

- An executive level crisis management plan that guides the process of responding to a disaster and allows executives to focus on their area of responsibility
- Formalized alternate modes of operation that can ensure organizational goals will continue to be met
- Trained personnel that are knowledgeable of their responsibilities in the event of an interruption

Business continuity will never be a silver bullet that protects the organization from every interruption, but it can allow an organization to make smart investments in protecting against the most likely and most severe threats.

Getting started

Starting any new process in an organization is challenging, but the key is always the same: have the right people involved and moving to achieve a central set of objectives. This often takes both time and diplomatic effort, so patience will be needed. Here are three key steps to getting a business continuity management process off the ground:

1. Understand Expectations

The best way to begin the conversation about business continuity is to have a conversation with your executive team about expectations regarding the organization's ability to respond to a disaster. Their response will probably be something like: "I think we're fine, our people are used to responding to a crisis

CONTINUED ON PAGE 20

CONTINUED FROM PAGE 19

and figuring out how to get product out the door" or "I haven't spent much time thinking about it, but I'm not sure we would know what to do or how to react." The criteria identified in the table below can be a guide to how other organizations like yours are approaching business continuity and provide some basis for why business continuity is important or how you should approach it. Many times, that's all that is needed to get executives interested in business continuity. With these expectations as a guide, the program will be supported by the executive team and provide the answers they are looking for.

CRITERIA INFLUENCING HOW MUCH TIME OR RESOURCES TO ALLOCATE FOR BUSINESS CONTINUITY

Public?

Organizations whose ownership is open to the public have the clearest mandate: protecting the business from unforeseen interruptions is part of management's fiduciary responsibility. If the board hasn't asked about the business continuity capabilities of your organization, it may be because they assume that it has been taken care of.

Private?

Medium and large private organizations should understand the expectations of their owners and explicitly document them. Many owners will expect that business continuity management is part of doing business, so expectations may need to be managed regarding current capabilities in this area.

Organization Size?

We recommend any organization or individual location with more than 500 employees conduct business continuity management. Smaller organizations will have less overall work to do, but even with 500 employees, having clearly defined communications, response and recovery expectations will increase the organization's ability to overcome a business interruption.

Industry and/or Regulatory Requirements?

Heavily regulated industries such as financial services and health care providers are expected to perform business continuity. However, many industries have begun widespread adoption of business continuity management, particularly manufacturing and pharmaceutical/bio-tech where customer demands have sped adoption.

Customer Demands?

Widespread adoption in the manufacturing and pharmaceutical industries is being driven through an increased focus on supply chain risk management and ensuring the continuity of products movement. Many customers are inquiring about their vendor's business continuity capability. This is especially true for companies which are sole source providers of critical products and services. Maintaining that enviable position will eventually require demonstrating an ability to persevere disasters.

2. Establish Accountability

Clear accountability for business continuity activities should be established to ensure their progression in the correct direction. This frequently resides under the CFO with a Director, such as Director of Risk Management or Insurance. Occasionally IT is given responsibility for business continuity; however, they often struggle with effectively connecting with the business.

3. Conduct A Pilot

When starting out with business continuity, most organizations conduct a pilot of one facility to understand the constraints and demonstrate the benefits of the program. Frequently, the pilot is the corporate headquarters so that senior executives can be involved and incorporated into the executive crisis management plan. Once the pilot is successfully deployed, the scope can be expanded to all facilities which house critical activities.

Conclusion

The use of business continuity management in organizations continues to expand and evolve in parallel with the broader discipline of risk management. Like risk management, business continuity management is a flexible process that is meant to be used in a way they best fits the organization. While using this process, each step will contain its own individual business case for continuing. As a result, the cost and benefit of business continuity management will vary from organization to organization. However, nearly all organizations should deploy some form of it to meet their obligations to stakeholders.

ABOUT THE AUTHOR

Robert Giffin is a Director and co-founder of Avalution Consulting. Rob specializes in the development of business continuity programs in the manufacturing, healthcare and consumer products industries, as well as in government. Rob can be reached via email at robert.giffin@avalution.com or at 800.941.0381.

WHEN 911 CAN'T RESPOND...

WHAT WILL YOU DO?

WILL YOU REGRET NOT HAVING SUPPLIES?




EMERGENCY LIFELINE CORPORATION

Take Action Today! We can help you stretch limited budget dollars to provide for:

- SEARCH & RESCUE
- MEDICAL RESPONSE
- EVACUATION
- FOOD & WATER
- SANITATION
- LIGHT & WARMTH
- COMMUNICATIONS

HISTORY

Emergency Lifeline was founded 23 years ago after the devastating Mexico City earthquake. Our mission then and now: to assist businesses, government agencies, schools and individuals prepare for any type of emergency or disaster.

Our supplies and kits can now be found throughout the United States and in many foreign countries! We are one of the oldest and largest disaster preparedness companies in the marketplace.

Be sure your supplier has the experience and judgment only time can buy!

EMPLOYEE DISCOUNT PROGRAM

For our institutional customers, we offer terrific discounts to their employees for personal purchases. After a disaster, a business needs their employees more than ever! But if they aren't prepared at home, they can't come back to work!

For complete product listings, contents lists of our kits, and much more, visit our website. Or call us today!

(800) 826-2201

www.emergencylifeline.com

THREE RECOVERY EXPOSURES YOUR ORGANIZATION IS FACING – AND YOU MAY NOT EVEN KNOW IT

BY REBECCA LEVESQUE

Growth and profit – it's the mantra of today's aggressive business executives. With market pressures mounting and stockholder value in the balance, busy executives continue to seek unique solutions to customer challenges in an attempt to establish competitive differentiation.

However, the very drive and ambition that pushes your organization forward may be putting you at risk. Many company executives we speak to put so much energy into the development of innovative infrastructures and environments to provide better service and greater customer insight that they forget about developing the strategies and tactics to ensure it can all be recovered.

The siloed approach separating business management and IT management often does not allow the insight into how IT departments are ensuring that critical business processes can continue after an event. Business managers don't require a crash course in IT management to see how their applications and data are managed, but they certainly should understand the opportunities and exposures related to recovering those critical resources.

John Morency, a research director at Gartner, has noted that "for many organizations, time required to recover critical business processes...has dropped by roughly an order of magnitude from what it was 10 years ago." We have seen similar trends; the business continuity market has notably shifted in the past few years, with greater focus on availability and recoverability, as well as intense interest in auditing and validation.

Identifying when and why

Data recovery strategies should contribute to operational efficiencies and business initiatives, as well as focus on shrinking recovery windows and aggressive Recovery Time Objectives (RTO)/ Recovery Point Objectives (RPO). Companies with truly effective data recovery strategies benefit from greater availability and reduced risks, as well as lower overall costs of recovery management. Effective data recovery strategies should provide a window into your actual application and data usage, and align your recovery management with real-world business challenges.

A business impact analysis (BIA) can help assess the business impact of data loss when a rapid recovery does not occur. However, it's important to note that the static nature of a BIA can prove to be problematic, especially if the analysis involves a high degree of speculation. As such, companies run the risk of missing the full impact of potential disasters.

In today's increasingly competitive and regulated marketplace, achieving an ironclad, dynamic data recovery strategy is the price of doing business. However, with the increasing costs associated with securing successful backup and recovery, accomplishing that goal is more difficult than ever. We believe that most recovery exposures can be separated into three categories; and if properly addressed, will significantly enhance recoverability.

1. 50% of all disaster recovery tests are unsuccessful

While most companies have documented recovery procedures for retaining and recovering information across the enterprise, those processes often fail during testing and real-life recovery efforts. According to Gartner, more than 50%

of all DR tests fail and 95% of all companies never complete DR testing. The primary reason for these failures is the lack of knowledge about physical and virtual systems, storage, applications and data, as well as their interdependencies.

In addition, many DR plans do not highlight the most critical and sensitive applications and processes that would be immediately required after an event. Therefore they do not prioritize those applications for immediate recovery so that the business can continue these operations. That means the critical applications and data you believe to be backed up and recoverable may indeed be a major exposure to your continuity.

Compliance requirements are often causing some of these challenges. Retention policies are often at the top of many compliance rules and audit requirements, and companies are turning to complex mirroring and redundancy efforts to ensure data is stored and secure. However, creating duplicate copies of all data also replicates any errors or corruptions. In addition, it can extend the time-to-recovery because all that redundant data needs to be recovered and restored – regardless of its importance or its impact on your business operations.

We always recommend a complete assessment of application and data interdependencies, especially as it relates to the most critical files and data your organization would need immediately following an event. That assessment needs to be very flexible, as the data sets you require on a quarterly, monthly and even daily basis may change often.

2. New technologies can actually increase your recovery risk

Many DR processes based on legacy systems have not changed in many years, so they do not include the newest applications and servers integrated to support new business initiatives. That means all the latest ERP, SFA or CRM applications you may have installed to improve customer insight or increase productivity may be at risk.

Applications and databases are often installed across multiple physical servers, and could be located in different physical locations. An event that disrupts the normal processing capabilities at any location will put your new application at risk. However, because DR plans are often only updated yearly, you may not even know the extent of your current exposure.

Even worse, the implementation of new IT initiatives like consolidation and virtualization that are intended to reduce operation and management expenses may actually cost more in business loss and compliance fines later on. Virtualization, which offers tremendous benefits by separating applications from their physical servers and providing greater management capabilities, can greatly reduce application recovery if not managed correctly. With many new and legacy application and data interdependencies scattered across multiple virtual machines, your ongoing recoverability is directly tied to your IT department's ability to track and manage those interferences.

The implementation of new IT initiatives like consolidation and virtualization may actually cost more in business loss and compliance fines later on.

3. Few companies can consistently prove they're recoverable

As we pointed out earlier, compliance regulations are causing havoc in the data center as well as the executive suite. Corporate and regulatory agencies often require proof that sensitive and critical data is recoverable as part of an overall compliance survey.

Most backup applications can provide a list of storage locations for backup data. However, focusing too strongly on auditing and reporting on data volumes – without obtaining access to the type of information that can provide real business value and insight – can prove to be problematic in creating a solid long-term business continuity plan. That's why the only proof some organizations can offer is to point at their mirror site with all their redundant data and plead for understanding.

In the wake of compliance requirements and the competitive exposures that come along with them, executives and business managers should have the ability to prove that their processes and workflow are recoverable through audits and verification reports that provide reporting on demand. That means establishing a documented process for monitoring critical applications and files, tracking their backup location, and providing a critical path for the immediate recovery of those resources when needed.

So where do you go from here?

Below are some key areas of concern to ensure your IT department is aligned with your business requirements, and is able to recover critical applications and data when needed.

- Can you identify critical applications?
- Is your most important information recoverable in an acceptable "business window"?
- Are you maximizing the utilization of your storage resources?
- Are you using mirroring or replication to its greatest efficiency?
- Do you know what is missing from your recovery process?
- Have you tracked where all your data is by key process – and how you plan to retrieve it in the event of an emergency?
- How do you handle data corruption vs. technology or environmental disruption?
- Business managers and executives can work together with the IT organization to address these areas and close the gap to recovery.

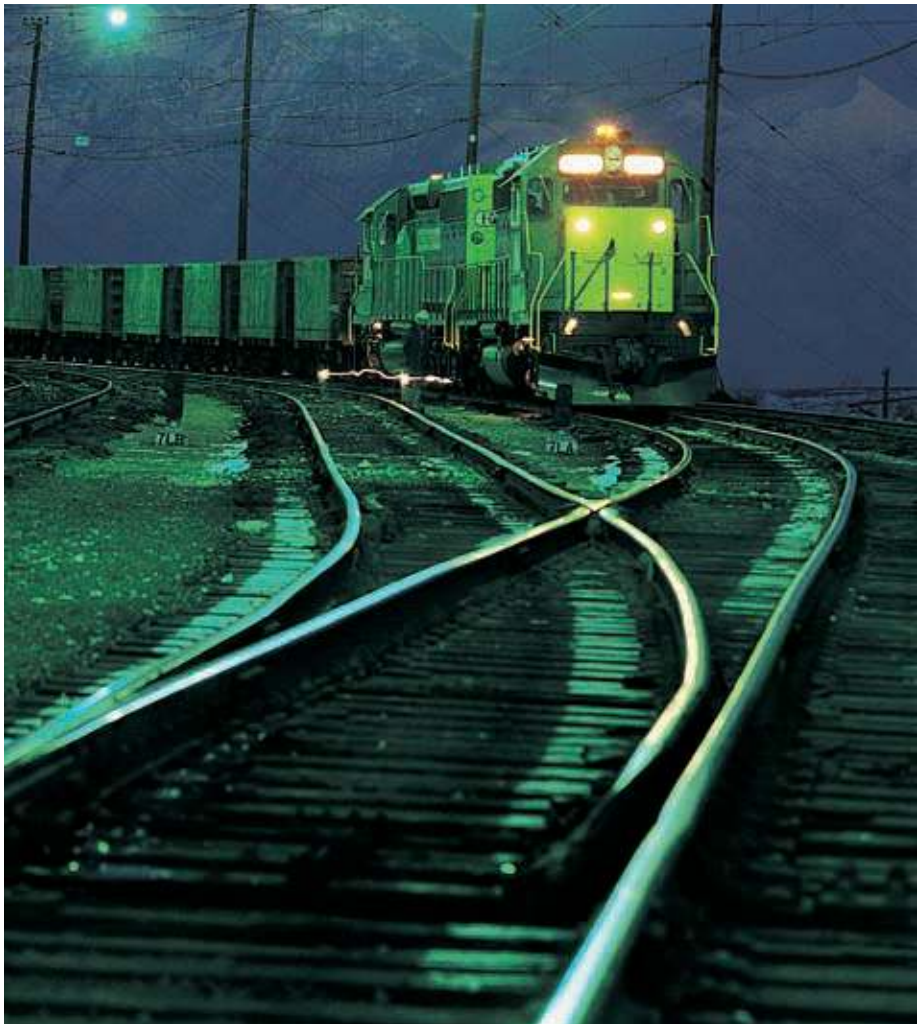
ABOUT THE AUTHOR

Rebecca Levesque is Senior Vice President of 21st Century Software (www.21stcenturysoftware.com). She regularly addresses many DR/BC related user organizations and enjoys sharing the benefits of her experience and exposure to a multitude of DR issues. She has spent over 15 years in storage management and disaster recovery with hundreds of client companies.

PLANNING FOR SUPPLY CHAIN CONTINUITY

BY DAMIAN WALCH

How resilient is your supply chain? Retail and manufacturing supply chains are becoming more complex every day. As they become more complex, the risk of disruption due to failure anywhere along the supply chain grows. The supply chain behind your neighborhood hardware store stretches across the world.



Factories, warehouses, shipping terminals and stores are vulnerable to the full range of natural disasters and the loss of critical resources such as people and power. Transportation services, with their assets everywhere on the road, may seem less vulnerable to catastrophic loss due to a natural disaster, but they can be crippled by labor actions in remote locations.

Supply chains typically involve a maze of third party suppliers, business partners, service providers and, of course, customers. Managing continuity risks in the supply chain is a process that inevitably involves working with these third parties to plan, execute and monitor continuity strategies. Supply chain continuity management is an emerging discipline. Nobody has all the answers, but this article will point to some good questions to ask and suggest a sequence for asking them.

Several business trends are contributing to a growing awareness of continuity risk related to the supply chain.

Low cost global sourcing has become a competitive necessity for most retailers and manufacturers. Even small and medium-sized businesses have global sourcing strategies. Global sourcing can increase continuity risk by increasing the overall level of complexity and by increasing the likelihood of disruptions caused by certain threats such as terrorism or by changes in the political or regulatory environment. The supply chain complexity brought about by global sourcing can also complicate and delay recovery efforts as, for example, communications delays can result from time zone differences, language or cultural barriers.

To be competitive, many supply chain enterprises are seeking to concentrate on outsourcing functions which a service provider can provide at lower cost and perhaps also with improved performance or effectiveness. IT functions such as web hosting, data center operations or application development are often

outsourced. Other supply chain functions which are typically outsourced include transportation, logistics and manufacturing.

While outsourcing is a proven method for cost reduction and quality improvement, it also adds to the complexity of the supply chain. It typically reduces the visibility and awareness of risks within the outsourced process. If not managed properly, outsourcing can slow down response times for disaster recovery or other supply chain events.

Supply chain managers have been working hard for years to apply LEAN management processes to reduce costs by minimizing inventory handling and storage and optimizing the use of factory, distribution center and transportation assets. To the extent they've succeeded, they've probably made the supply chain more sensitive to supply disruptions by reducing the tolerance for error. As more integration is achieved between the supply chain processes of different companies, the impact of a supply chain disruption is likely to become greater for all parties.

What are my business requirements for supply chain continuity?

Planning for continuity in the supply chain will ultimately involve working collaboratively with suppliers and other key business partners. Before we get in a room with them, however, we need to determine our own requirements. Do a business impact analysis, identify and prioritize your supply chain processes and determine your recovery time objectives.

Where does my supply chain begin and end?

Map the supply chain from raw materials to the customer. Ask the questions, get the answers and document the results. Answering this question may not be as simple as it may seem at first. We know our suppliers, but do we know their key suppliers? Are they sole-sourced or multi-sourced? This mapping effort can begin right away, but it probably won't be complete until we've gathered information from suppliers and other business partners.

A supply chain can be thought of as a network of manufacturing centers, distribution centers and stores connected by transportation services that manage a flow of goods. Suppliers on this network will include raw material providers, component or contract manufacturers, transportation carriers and third party logistics providers (3PLs).

The network that supports the flow of goods is not the only network involved in the supply chain. There is also a flow of information and communications for order and procurement processing supported by data centers, and voice and data communications links. Suppliers on this network will include telecommunications carriers, application service providers, IT outsourcing providers and even disaster recovery service providers such as hot-site vendors.

All the networks and the nodes that support them must be resilient.

Who are my key suppliers of goods and services?

Emphasis on "key". With a map of the supply chain in front of us, it's time to determine which suppliers are important for continuous business operations. What risks do they represent? How are we impacted if this one or that one fails? We will want to work closely with the key suppliers as we move forward with business continuity planning.

With key suppliers identified, estimate the probability for a supply chain disruption or business failure. Many suppliers will potentially be assessed so it is important to establish a consistent analytical method for analyzing the potential for disruption and the likely impact of the failure. Apply the same method or analytical framework to all key suppliers. Consider the current relationship with each supplier and the contractual, procedural and technical controls in place that contribute to continuity.

Is my sourcing strategy a fit for my business continuity requirements?

Not all suppliers are key suppliers and we will manage supplier risk in more than one way. Commodity supplies might best be procured from multiple sources. Multi-sourcing not only encourages price competition among commodity providers, it also provides fall-back options in the event of a failure of one supplier. A given commodity supplier can still be considered a "key supplier" if it accounts for a high volume of business or it otherwise represents a significant risk to the supply chain. Alternative sources, however, represent a viable mitigating strategy.

Multi-sourcing isn't always the answer. Many companies turn to sole-source suppliers for highly engineered parts or supplies where a high level of quality control is essential. These sole-source relationships represent business partnerships which must be managed carefully and proactively for supply chain continuity.

What are my key suppliers doing about business continuity?

With our own business continuity priorities understood and key suppliers identified and profiled, we need to work with key suppliers to understand their business continuity capabilities and to identify gaps between that capability and our own needs. Many companies use detailed questionnaires which cover all traditional domains of business continuity capability including organization, governance, business impact analysis, business continuity strategies, awareness and training programs, incident response, and crisis management procedures and documentation.

Can we survive a crisis together?

Crisis management is an essential part of any business continuity capability. Essential elements of a crisis management capability include the following elements:

Trained local emergency response teams with defined roles, procedures, and communications protocols for emergency response.

A pre-arranged command center where key decision makers can be joined with a communications hub.

An executive crisis management team with roles and responsibilities identified for specific processes such as supply chain coordination, employee coordination, and media communications.

CONTINUED ON PAGE 26

CONTINUED FROM PAGE 25

In a supply chain it is important for supply chain partners to be able to work together closely during a crisis. Channels for communicating and sharing information with supply chain partners must be established – or re-established – in the event of a crisis. Contact lists with crisis management roles and responsibilities are needed on both sides of the relationship. In some cases, supply chain partners may have a seat in the command center. Supply chain partners talk about the importance of a "shared situational awareness" for all organizations involved.

How can I work with key suppliers and service providers to achieve and sustain my required level of continuity?

A joint business continuity planning effort with key suppliers is an excellent start. But the ultimate goal is to integrate business continuity goals and objectives into existing supply chain processes. For example, suppliers should be answering questionnaires about business continuity capabilities as soon as they become candidates during procurement selection. Contracts with suppliers can mandate the periodic review of continuity controls. An updated assessment of business continuity capabilities can be part of the periodic supplier scorecards in vendor management.

A basic reality for all business continuity planning extends to supply chain continuity planning: if it's not regularly reviewed and tested, it's not real. Supply chain partners must work together to periodically review and test their joint disaster recovery plans and other elements of the business continuity capability. This is another understanding that can be built into the contract but it ultimately needs to become integral to the culture and expectations of the extended organization.

How can I build resilience into logistics processes?

Supply chain continuity is one aspect of a broader category of issues called Supply Chain Risk Management (SCRM). Consultants and trade groups can help with a range of best practices for supply chain management and these include methods for building resilience into the supply chain.

A strong partnership can make the difference between survival and total catastrophe in the event of a disaster. Transportation carriers often have experience helping retail or manufacturing customers weather a disaster. Truck carriers, for example, can turn a secured parking lot into an interim warehouse simply by parking trailers for an extended period of time while distribution centers or stores are in recovery. Many carriers offer logistics services and can provide temporary warehousing space on short notice. Some carriers can even leverage their other business relationships by arranging for storage space from their other customers while the primary customer is recovering from a lost distribution center or store.

When a disaster occurs, partners in the supply chain are in a better position to leverage each others' operational capabilities if advance planning has been done to define contacts, roles, contingency communications tools and methods of information sharing.

Integrated networks and information systems can greatly accelerate logistics recovery efforts. With development effort, companies with centralized, integrated warehouse management systems can script all the routing changes necessary to compensate for a lost distribution center, reducing a major part of the recovery effort to a single mouse-click. When a regional warehouse is disabled, the script instantly routes all deliveries from alternative, neighboring warehouses according to the SKUs available at those warehouses and the routes needed for delivery.

Summary

A good planning process for supply chain continuity begins with asking the right questions. A strong supply chain continuity capability ultimately relies on strong, well chosen and well managed business partnerships with an environment that enables management and staff from all organizations to roll up their sleeves and work together during a crisis. The benefits of a strong continuity program include stronger partnerships overall and a greater potential for business success going forward.

ABOUT THE AUTHOR

Damian Walch is a Director with responsibility for delivering technology recovery and business continuity services. This 18 year veteran and frequent speaker was named to Consulting Magazine's 2003 Top 25 Consultants of the Year. He can be reached at dwalch@deloitte.com.

June 15 – 18, 2008
Toronto, Canada

18TH WorldConference on Disaster Management

Resiliency – Individual, Community & Business

Networking on a Global Scale

Register at www.wcdm.org

Save $200 off Full Conference Pass with Priority Code: DRG08

Be a Sponsor. Be an Exhibitor. Be a Participant.

905.948.0470 x 246 | Toll Free: 888.443.6786 x 246

Conference location:
Metro Toronto Convention Centre

Presented by:
The Canadian Centre for Emergency Preparedness: www.ccep.ca

Working Together
Business Continuity and Emergency Management

INTERDEPENDENCIES – A KEY ASPECT OF CONTINUITY THAT EXECUTIVES NEED TO UNDERSTAND

BY JOHN A. JACKSON

Interdependencies between an organization and other business partners and public agencies have always been an overlooked or at least under-served aspect of Disaster Recovery and Business Continuity plans. This article serves to raise the awareness of this important issue to the executive suite, so that executives can ensure it is being properly addressed.

The Changing Face of Disasters

Most organizations have long been aware of the business impact of an unplanned interruption to business operations, most probably including an outage to computer and communications based systems. The events of the past several years, including 9/11 and Hurricane Katrina have raised those concerns to a fever pitch, and have highlighted a number of previously under-considered aspects of contingency planning, including:

- The impact of a loss of personnel
- The potential to have operations disrupted due to a geographic impact which eliminates building access even though no direct impact occurred
- The potential for a loss of paper records and the need to rely solely on the inventory of an offsite storage facility, most probably only containing electronic data backups
- The realization that the company's primary workplace could be permanently destroyed, requiring the acquisition of, and outfitting of a new base of operations before recovery can occur

In addition to the above, many organizations now realize that most disasters require that companies not only focus on their own individual recovery plans, but they must also consider how the recovery efforts of other companies in their industry, as well as customers, suppliers or supporting industries must be coordinated so that normal, or near normal operations could resume. They also now realize the impact that outages of the public infrastructure or the actions of public agencies or officials could have on their individual or collective abilities to recover.

The Business Continuity Industry Today

The past history of the business continuity industry is one where the recovery facility vendors (those who provide facilities and equipment to facilitate recovery) focus on discrete contracts for individual companies. These contracts are not synchronized, in almost any way, with those of other firms that could be required in order for an industry segment or geography to recover. Essentially, the recovery industry vendors offer services that provide recovery facilities, network connectivity and equipment for individual companies to use, assuming no conflict with another customer that prohibits access

and use. While that strategy has served well over the years, a more comprehensive strategy might now be required due to the potential for disasters to impact more than one organization at a time.

Any organization that approaches the topic of business continuity typically goes through approximately four sets of activities. While methodologies vary among vendors and companies, the following overall process is typically undertaken.

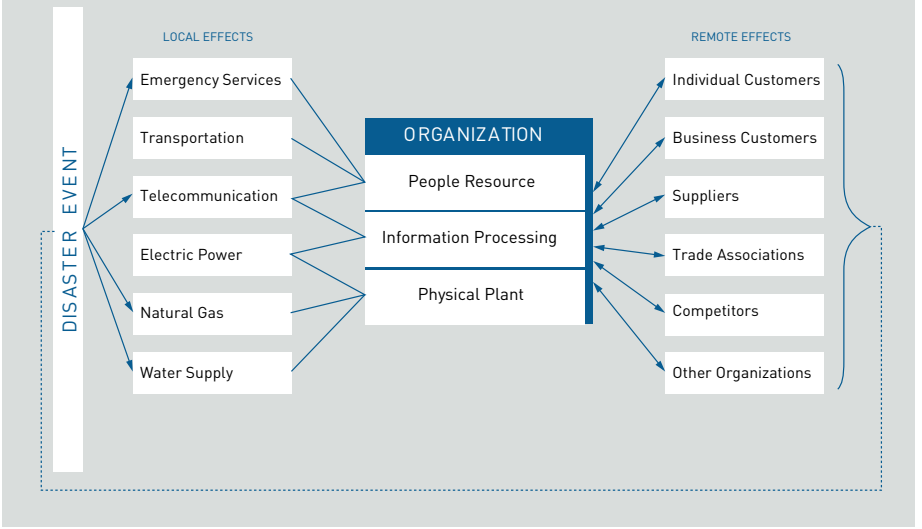
1. Business Impact and Recoverability Assessment: Determining the Risk
2. Recoverability Strategy Development: Setting the Course
3. Strategy Implementation: Putting the Solution In Place
4. Plan Maintenance and Testing: Making Sure it Works

This four-step process starts with the first step, the business impact analysis. This process, often carried out by experienced continuity consultants or internal company resources, is designed to understand the financial, contractual, regulatory and legal impacts to an organization, of an unanticipated interruption to their business (offices or computer systems) operations.

The BIA effort, which helps to determine the organizations recovery time (time to recover) and recovery point (protection of critical information), focuses on an individual company's needs but generally disregards the impact on other organization's. Two or more organizations, in the same or reliant industries, might have totally different recovery times and points, and not know it until they both would go through the recovery process. This occurred in New York during Sept. 11, 2001, when many organizations found that their plans were either short sighted or more comprehensive than others, and their recovery efforts were delayed until the organization with the lesser plan (generally a longer planned recovery time) was ready. Essentially what occurred was that the "weakest link" scenario was played out.

The issue of interdependencies has highlighted that the current BIA process does not go far enough, either for an individual company, or now, as important, for the authorities to gauge a complete picture of how an industry or business district would be affected. Essentially, what individual organizations need to ensure is that the BIA process focuses on geographic (building or metropolitan area) or industry recovery, not just their individual business.

ORGANIZATION INTERDEPENDENCIES



Conducting an Interdependencies Exercise

Given the issue of interdependencies and the inherent shortcomings of the BIA process, some forward thinking experts are now suggesting that organizations conduct an "Interdependencies Workshop" to ensure that both private industry and public agency interdependencies are considered in the planning process.

The interdependencies workshop is intended to understand the interdependencies of business to business interactions and reliance's, as well as local physical infrastructure components and the effect of an outage on firms in a given geographic area, should a terrorist or other crippling disaster scenario occur. It is vital that private organizations consider this issue during this initial phase of recovery strategy development. Organizations that must be considered for their interdependence include other major businesses, communications, electric power, oil/gas, water, and transportation providers, as well as government services, hospitals, and any other major service suppliers.

The above graphic illustrates the interactions which must be considered during an Interdependencies Workshop exercise.

The interdependencies workshop is an important first step leading to a focus on the recoverability of companies and governmental agencies outside of an individual companies' purview, from an information protection and business infrastructure (offices, computers, phones, personnel) point of view.

The results of an interdependencies exercise would include:

- A high level understanding of critical resources which might impact an organization's ability to recover in a timely manner
- Organizational awareness of weaknesses in business recovery strategies
- Development of a matrix listing identified weaknesses, so those weaknesses can be addressed
- A clear understanding of the high level contingencies currently in place

Spreading the Word

Currently, there are a number of organizations bringing focus to this important issue. In the Chicago area, ChicagoFirst (www.ChicagoFirst.org) has been formed to bring together members of the financial industry to promote awareness of interdependencies and each organization's interface with public agencies. The ChicagoFirst model has been so

CONTINUED ON PAGE 30

CONTINUED FROM PAGE 29

successful that it has spawned similar groups in other cities. A national organization focused on this issue is the FBI-sponsored InfraGard (www.infragard.net). They have national chapters which promote meetings between private companies and public agencies, aimed at developing a better understanding of each other's needs and capabilities.

ChicagoFirst and InfraGard are but two of many organizations focused on this issue. Private and Public Businesses Inc. (www.ppbi.org) promotes focus through classes on related topics and the recently formed Lake Cook Critical Infrastructure Partnership in Northern Illinois has made great strides in pulling private industry, local fire, police and emergency management and national organizations like DHS together to focus on this topic.

Summary

The concepts outlined in this article present an approach to dealing with the fact that most, if not all recovery plans, are stand-alone islands. Most plans do not address the inter-relationship of the recovery times and the recovery points of organizations a company or agency relies upon and interfaces with. Most plans also do not take into account the regional effects on public infrastructure and how that might affect the ability to recover in a timely manner. Company executives should ask if their recovery plans and strategies address interdependencies and require that this aspect of recovery be addressed.

ABOUT THE AUTHOR

John Jackson has 30 years of IT Risk Management experience and is a well known leader in the Business Continuity industry. John is currently Executive VP of Fusion Risk Management. Previously, he was General Manager of IBM BCRS, an SVP at SunGard and President of Comdisco Continuity Services. John is also the Chicago Chapter President for InfraGard, focused on Private and Public partnerships.

SPONSORING COMPANIES

DISASTER RESOURCE GUIDE

Published by Emergency Lifeline Corp.

PO Box 15243
Santa Ana, CA 92735
Tel: (714) 558-8940
Fax: (714) 558-8901
info@disaster-resource.com
www.disaster-resource.com

Executive Publisher: **W.T. Rainey**
Publisher: **Kathy Gannon Rainey**
Editor: **Alison Dunn**
Directory Coordinator: **Carlos Rincon**
Production Coordinator: **Daniel Herrera**
Advertising Sales: **Everett Troy, Clayton Bauland**
Circulation: **Carmen Plascencia**
Office Support: **Elizabeth & William Rainey**

PRODUCTION CREDITS

Luis Alvarado Design
– Luis Alvarado
– Trina Werkema

ON THE WEB

Visit the Online GUIDE. Lots of good information! Exclusive Online Articles, What's New, Industry Briefs, Meet the Pros, Purchasing Priorities and much more!
www.disaster-resource.com

Disaster Resource GUIDE – Volume 12 Issue 3, March 2008 – is published quarterly (March, May, August and November) by Emergency Lifeline Corporation, 1510 East Edinger Ste D, Santa Ana CA 92705 and mailed/distributed to qualified individuals who have requested a copy and who have oversight or responsibility for business continuity, enterprise risk, crisis management, emergency response, and/or homeland security. Individual copies are available for $20.00. Application to Mail at Periodicals Postage Rates is Pending at Santa Ana, CA, and Additional Entry Offices.

Postmaster: Send address changes to
PO Box 15243, Santa Ana, CA 92735.

Digital Phone & Fax
Real Time Video
Two Way Radio
Broadband Data

ON SCENE & IN TOUCH

WITH SATELLITE COMMUNICATIONS

Rapidly deployable on-scene communications are crucial for law enforcement and emergency response personnel. With over 25 years of experience, Spacenet offers a field proven portfolio of transportable satellite solutions for complete communications. Easy to use push-button systems provide carrier class digital telephone and fax service, broadband Internet access, two-way video and even land mobile radio support. Whether deployed for just a few hours or on a relief effort lasting weeks, some of the nation's largest commercial and government organizations depend on Spacenet for their critical communications.

For more information visit www.spacenet.com or call 866.480.2263.

The High-Performance Choice for Non-stop Networking™