

Business Continuity

Are You Prepared?

Strategies, Products, and Services for Today's World

By, Cheryl Krivda

The concept of preparing for potential business disaster is nothing new, except that everything is different now. Years ago, companies weighed the consequences of "standard" threats such as fire, flood or earthquake—not business-stopping power outages, production-halting supply chain disruptions, trust-busting Website compromises or facility-destroying terrorist acts. A decade ago, continuity problems were costly, but—except for rare, truly catastrophic events—recovery was usually possible. Now, with global, around-the-clock operations and real-time everything, even minimal disruptions to business continuity can be financially crippling or fatal.

These "unplanned changes," as continuity experts call them, can negatively impact a corporation in several ways. Crises can jeopardize lives and safety, making employees unavailable. They can also endanger customer relationships or short-circuit business operations; disruptions can imperil the corporate image and challenge regulatory compliance.

As a result, business continuity planning (BCP) is no longer a task executed only by wary IT leaders or cautious risk managers. Ensuring business continuity is the fiduciary and managerial responsibility of every corporate executive. Nor is business continuity a luxury, affordable only during economic good times. Like insurance, BCP is an expense that can protect against tremendous loss. It is a critical investment that, well-chosen, can deliver incomparable payoff. So how should executives select the appropriate continuity options?

Choosing Wisely

Within the broad category of BCP are three discrete approaches to protecting against unpredictable business threats: continuity planning, recovery preparedness and risk management. Continuity planning addresses the steps taken to minimize the impact of uncontrollable conditions, such as installing generators to handle basic, short-term or emergency electrical needs during a power outage. Recovery preparedness covers the issues that can help an organization recover from crisis conditions, such as engaging a hot site where mirrored computer processes can run, should the home facility become inaccessible. Risk management reduces the likelihood of potential crises by taking steps such as training employees how to work safely, changing processes to reduce injury or implementing protective devices such as smoke detectors. Risk management can also include insuring the corporation against loss with policies that can protect against everything from physical damage to data loss and e-commerce breaches.

Executive Engagement

To protect the enterprise most effectively, these three approaches are used in concert. Yet a full-blown BCP program requires executive commitment to ensure that the corporation is prepared to deal with any eventuality, and this can be costly.

However, careful quantification of the organization's risks, potential loss due to crisis, and costs of buying continuity products and engaging services can create measurable return on investment. But even having concrete ROI numbers does not diminish the need for true senior executive-level buy-in to the value of BCP. Without executive backing, continuity tends to fall victim to budget battles and corporate politics. When top leaders endorse the need for adequate business continuity preparations, enthusiasm for BCP spreads throughout the organization. Continuity assurance becomes a responsibility for all employees—creating a more secure, prepared and recoverable enterprise.

Because continuity must be addressed across the enterprise, it cannot be relegated to any one department or division. In fact, some organizations are driving the success of their BCP efforts by making continuity a separate line item in the corporate budget. "Delineating BCP financially helps organizations address it as an enterprise concern, with impact across the business," says Brian Turley, president of BCP vendor Strohl Systems Group. "We've even seen some companies putting BCP readiness into the performance reviews of their key managers. This is another effective way of making sure business continuity becomes a main focus."

Protecting the Enterprise, Effectively

Despite the long history of disasters that have destroyed businesses, the practice of BCP is a relatively new discipline. The number of broadly trained continuity experts is small, and most of those people work for product and service providers. Getting someone with relevant expertise on your staff is difficult, and can be costly.

Therefore, executives must be prepared to cultivate a network of continuity experts from among providers serving the business market. These experts can help business leaders consider strategies and tactics for assuring continuity, and can provide a wealth of information on the acquisition and application of hardware, software, and consulting services.

Unlike previous generations of continuity services, which stressed tactical preparation for specific disasters, today's experts tend to think strategically, designing comprehensive mitigation of, as well as responses to unspecified, unplanned change. In addition to planning concrete recovery processes, organizations are also recognizing the need for business processes required to support recovery. Planning continuity from a business perspective instead of an IT or data perspective enhances results.

"Tactical BCP methods try to anticipate which problem might occur and how the company would respond," explains Dr. Don Saracco, executive vice president and COO at MLC & Associates, Inc., a consultancy focused on strategic continuity assurance. "In today's world, it makes more sense to think about making a company more prepared strategically. Usually that means creating a robust organization and developing a competent employee workforce that can meet any challenge."

Strategies for Success

Designing and refining the organizational plan is critical to the success of continuity assurance.

Unlike other documents, which are created once and can serve as an ongoing reference standard, the business continuity plan is a living document. Created by a process of internal assessment of business processes and resources, in order to remain useful, the plan must be reviewed and updated as conditions change.

For example, the terrorist attacks of September 11 caused many executives to review and rethink their continuity plans. A recent Booz Allen Hamilton survey of 72 chief executives found that since 9/11, 74 percent had reviewed their insurance policies and 90 percent had reviewed their continuity plans. But dramatic events such as terrorist attacks are not the only changes that warrant ongoing development and review of the continuity plan. At Toyota Motor Sales, U.S.A., Inc., headquartered in Torrance, CA, business continuity is a mature discipline that includes regular reviews and updates of its plan.

In 1997, Toyota combined its business continuity planning and emergency response organizations into a unified disaster management team. The team is part of the company's Safety and Environmental department, reporting to corporate through the administrative services division. With the goal of insuring the safety of associates and the continuation of its business nationwide, Toyota's disaster management team mission is to "maintain the optimum state of disaster preparedness through planning, preparation, training and exercise."

Positive Opportunity for Change

On the planning front, the company updates its continuity plan twice a year to reflect changing personnel and business processes. "It's an ongoing cycle," says Janet L. Mebust, business continuity manager. "Our executives understand the need for a continuous process of development, refinement and improvement."

In addition to plan development, Toyota stresses corporate continuity training. All employees participate in semi-annual evacuation drills. Nearly 1500 employees have been trained in emergency preparedness as part of the Corporate Emergency Response Team (CERT). All training takes place on company time.

"Training our workforce is just common sense," says Mebust. "Regardless of the size of a corporation or its success, everyone is vulnerable to disaster. We have a responsibility to our employees, our communities, and our business partners to ensure we are as prepared as possible to deal with whatever difficulties we may face."

Duplicate and Disperse

Beyond planning, a corporation's continuity strategy must incorporate specific hardware and software products. Because many vendors build products based on specific continuity strategies, buyers should understand how they mesh with the corporation's continuity plans. For example, some storage and backup technologies support the strategy known as "duplicate and disperse." This strategy encourages corporations to duplicate data so that it is available in geographically dispersed locations. In the event that one location or even region is inaccessible, data can be accessed at another location.

For crises that prevent staffers from being able to work, some products offer automatic messaging and centralized remote management. "People and information are the two most important assets to most organizations," says Stephen Higgins, director of marketing for business continuity at EMC. "But often, recovery must occur without people, because they cannot get to the physical location, for example." Automatic messaging enables certain basic recovery procedures to execute without human intervention, minimizing continuity disruption. Centralized remote management enables authorized managers to restore systems and data from remote locations.

Productive Protection

For corporations concerned about the cost of protection, some continuity products are designed to do double-duty, maximizing their effective usability. EMC advises customers to use mirrored data systems at remote sites supporting data warehousing, application development, or customer relationship management processes.

Instead of backing up data to a hot site where it sits idle, says Higgins, EMC products convert the backup site to an active asset. "This type of architecture really brings down the total cost of ownership for the protection," he says. "The impact can be huge."

Selecting Software

Software products in the BCP market generally handle either continuity plan development or business impact analysis. When selecting a planning solution, buyers should look for a complete package that includes a powerful relational database. The database stores not only the plan document, but also any links to business processes, organizational departments and vendors mentioned in the plan. This is critical for keeping the plan current and establishing effective change control.

"When large companies develop a complete continuity program, their plan documentation can be extensive," says Strohl Systems' Turley. "If one vendor is replaced, it can create dozens of changes throughout the plan. Having a planning product that updates those references automatically simplifies maintenance and guarantees accurate change control."

Other software products help businesses determine the operational and financial impact of crisis. What assets will the organization need, and when? By answering questions and working through scenarios posed by the software, planners can anticipate the cost of crises over time and focus resource priorities accordingly. Understanding these costs and priorities can also help create senior-level buy-in to the continuity program. "When executives understand the financial impact of the disaster, it makes it very easy to understand the value of their BCP investment," says Turley.

When choosing one of these products, investigate the expertise of the software vendor and the vendor's development team. Some handle continuity concerns only as a sideline to other business issues; others have only recently entered the continuity market. Certain vendors can provide only

one type of software, while others offer integrated suites backed up by consulting services.

Network Communications

Of course, as the BCP market evolves, it is influenced by the crises encountered by businesses. No disaster has had greater impact on the way continuity is viewed than the terror attacks of September 11. Whatever strategies and plans corporations had in place before that day must be reconsidered in light of those events. Ron Vidal, senior vice president for Level 3 Communications

Vidal spent seven weeks at Ground Zero helping Level 3 customers, as well as other carriers and their customers, resume business operations. In the aftermath of this experience, he says executives must consider new continuity strategies that disperse operations, rather than centralizing them in one building, or even one region. For maximal protection, business processes, data centers, personnel and resources should be dispersed to diverse physical locations. Some corporations are even wondering whether to retain business operations in metropolitan areas or move them out to suburban locations that might be a less likely target.

Yet dispersing operations or resources requires additional communications among employees, business partners and stakeholders. If colleagues can no longer communicate face-to-face because they are miles or time zones apart, they need powerful communications networks to facilitate information exchange. Executives must look for communications networks that offer rich, multimedia functionality, deliver high availability and bandwidth, and support a robust communications infrastructure within metropolitan areas and their suburbs. "Today, companies rely heavily on communication networks to conduct their businesses; going forward, they will be even more tightly interwoven into the fabric of businesses."

Consulting with Experts

Clearly, the rising stakes for business continuity will encourage many organizations to engage outside expertise. Consulting services are broad, and include education, business impact analysis, building and maintaining a plan, and risk analysis. Some consultants specialize in discrete aspects of the BCP market—such as testing the continuity plan or handling crisis communications—while other organizations are deep enough to address a wide range of continuity issues. Look for consultants who are certified BCP professionals, preferably those with at least five years of experience. Many talented continuity professionals have backgrounds in the military, the public sector, and law enforcement. To handle cross-enterprise continuity concerns, seek a consultancy with a broad portfolio of expertise.

Consider an organization with front-line experience, staffers who have been through real crises, as well as those with organizational development skills and focused disaster recovery-planning capabilities. Consultants who understand change control, have executive and managerial experience, possess an IT background, or have worked on total quality or process improvement initiatives can also be beneficial. Experts with strength in customer service can be especially valuable, since ongoing communications, requests and solutions are common in resolving continuity issues.

The Human Touch

In continuity planning, beyond all of the products and services, executives must factor in the most important asset of the business—its people. One critical element of this planning is crisis communications. When even the unimaginable happens, the executive team must be prepared to communicate realities, plans and actions to a variety of audiences—including employees, business partners, stakeholders, the media and the surrounding community.

Every message communicated during a crisis must consider the human needs of the audience—even if the audience is varied. Regardless of the high-stakes situation, employees need to feel safe, stockholders want to hear how the company is protecting their investments, and a corporation's neighbors need proof that the business is acting in the best interests of the community. And although executives cannot anticipate every contingency, they can develop communications plans that address broad types of scenarios and define the corporate spokespeople, audiences and messages needed to recreate order from chaos.

Because most companies don't think about how they will communicate under emergency conditions, they often do it poorly. "A big problem during crisis is that corporations often forget to put a human face on the problem, and they speak like corporations," says Elaine Gansz Bobo, president of C4CS, a strategic communications firm specializing in crisis situations. "And failure to recognize these human elements can lead to colossal failure for the corporation overall."

How Much is Enough?

Deciding how much to invest to reduce risk is the calculus of continuity planning. Corporations are faced with a daunting task: trying to plan for and minimize the risks caused by unforeseen events. In a world where even minutes of downtime can result in hundreds of thousands of dollars in lost revenue, executives must prioritize their critical business processes, quantify risk and make investment decisions that assure the continuity of their business.

"Keeping an enterprise running at peak performance requires more than the conventional back-up tapes and cold sites," says Jo-Ann Mendles, Vice President, AT&T Business. Traditionally, most continuity planning has been relegated to the domain of the technologist, limiting back-up plans to telecommunications and computing. But today, corporations need to provide continuity for critical business information and processes. The "tools" include network availability, mirrored data storage and data centers, computing clusters, and replicated databases.

"Corporations require a continuum of continuity options with diverse IT infrastructures, HR contingency planning and physical logistics preparedness as key components of their continuity plans. Today's continuity solutions providers can develop a plan to transform the way an enterprise operates in the face of the unforeseen. Experienced providers can optimize the corporation's investment and develop a highly available infrastructure that fits the budget, and precisely matches the company's risk tolerance," says Mendles.

MLC provides comprehensive, integrated, disaster recovery and business continuity programs that mitigate risks associated with disasters, personnel disruptions, electronic attacks, and competitive threats by addressing:

- Operational risk—MLC develops customized contingency and business continuity plans, network designs, and systems security safeguards for protection against physical disasters and Web-based attacks;
- Intellectual property risk—MLC documents/ redesigns critical processes, develops personnel contingencies, and reviews patent and copyright protection;
- Financial risk—MLC reviews insurance programs/ develops related financial and operational recovery contingencies.

MLC has worked exclusively in DR/BCP for the past 15 years and is one of the world's leading experts, with credentials ranging from Fortune 1000 Companies, to FEMA/DOE policy work, to chairing the Association of Contingency Planners. MLC also audits existing plans.



BMS Catastrophe provides a complete array of recovery services designed to deliver the best available solutions for our clients. This leadership position has fueled significant growth for BMS CAT and has increased our capabilities in meeting recovery needs in virtually every corner of the world within hours of a disaster.

BMS CAT is staffed with expert personnel who deliver a full range of services. A single phone call will deliver a complete portfolio of professional personnel and services to meet your disaster recovery needs at a competitive price. Whether you need one service or have multiple recovery needs, BMS CAT is "Your Partner in Disaster Recovery."

Services

- Mold Remediation
- Dehumidification
- Document & Book Recovery
- Electronics & Information Medi
- Fire & Smoke Damage
- Water Damage
- Project Management



Level 3 is an international broadband infrastructure and communications company headquartered in Broomfield, CO. The company offers a wide selection of services, including IP services, broadband transport, collocation services and the industry's first Softswitch based services.

Level 3 built and operates the world's most advanced international multi-conduit, upgradeable network optimized end-to-end for high-performance IP packet switching technology. The combined U.S. and Pan-European network totals approximately 21,600 miles, including metropolitan networks in 36 cities, and is interconnected by a high-capacity transoceanic cable system.

Level 3 continues to develop collaborative relationships with customers to enable them to keep pace with rapidly changing technology and the needs of their own core customers. The network makes possible the use of a proprietary provisioning system that can deliver bandwidth in days, rather than weeks or months.