



Achieving Resilience – Best Practices in Business Continuity

Executive Summary

In 2002, AT&T instituted a long-term program designed to identify best practices in Business Continuity planning (BCP). As a part of this program, the AT&T Foundation made a series of educational research grants totalling \$250,000 to five U.S.-based universities. Their objective was to identify a more formalized approach to BCP that would help organizations identify and quantify risks and then implement procedures, strategies and tactics aimed at ensuring business continuity.

Each of the five universities focused on one of five vertical industries:

- Financial Services: George Mason University, Virginia
- Manufacturing and Supply Chain Environments: Michigan State University
- Pharmaceutical industry: Stevens Institute of Technology, New Jersey
- Retail industry: University of California, Los Angeles
- Travel and Leisure: Georgia Institute of Technology

Utilizing detailed case studies and surveys, each of the five papers explores areas such as strategic planning, risk assessment, back-up plans and work processes, continuous testing and industry-specific best practices. The research papers also provide several proposed frameworks for developing business continuity plans and questionnaires for self-assessment.

This white paper, written by AT&T in co-operation with the Economist Intelligence Unit (EIU), summarizes the key findings of the research. Three main themes emerged:

- The news media headlines may focus on single catastrophic events, but smaller, more mundane risks are responsible for more business disruptions. As a result, companies are shifting their focus from disaster recovery – the restoration of damaged assets – to business continuity planning – the uninterrupted provision of operations and services to end-user customers.
- Information technology dominates thinking on BCP, and industries that are heavily dependent on IT tend to be furthest along the BCP path. But IT should not push aside other elements of BCP, such as communications with employees, alternative work processes and interaction with customers.
- A static business continuity plan will not protect a company from disruption. An integrated and ongoing enterprise-wide plan, with assumptions that are regularly tested and that keep pace with the risks prevalent in the business environment, is needed to achieve this goal.

An Accumulation of Risk

The relentless rise of risk on the corporate agenda over the past few years has largely been propelled by a series of high-profile events – the Y2K threat, SARS, the war in Iraq, corporate governance scandals, the blackout in the northeast U.S. and a growing litany of terrorist incidents. Such events constitute the ultimate challenge to a business's ability to keep operating and dominated much of the early thinking behind “disaster recovery” processes, a term used to refer to the restoration of specific assets, such as data networks, following an operational disruption.

The good news is that the increased use of information technology, the globalization of supply chains and the integration of networks of companies into “extended enterprises” have helped reduce companies’ exposure to a catastrophic “single point of failure” disaster.

The good news is that the increased use of information technology, the globalization of supply chains and the integration of networks of companies into “extended enterprises” have helped reduce companies' exposure to a catastrophic “single point of failure” disaster. An extended geographic footprint and an increase in information flows within and between businesses mean that companies can diversify and manage risk more effectively than ever (for more on this topic, see *Networking and Business Strategy*, an AT&T white paper published in May 2003.)

The bad news is that these same trends can spawn less dramatic but equally damaging risks of their own. As more enterprises rely on extended supply chains, for instance, managers are coming to realize the true impact of supply-side disruptions. “Business failures, disruptions or shutdowns among a firm’s partners or in its inbound logistic channels can easily create a ripple effect of business interruptions throughout the supply chain, not unlike the results of a disaster,” says Dr. George Zsidisin, assistant professor of marketing and supply chain management at the Eli Broad Graduate School of Management at Michigan State University.

Similarly, the critical importance of information technology means that severe damage, both in terms of lost revenue and customer dissatisfaction, is inflicted when networks fail. At the New York Stock Exchange, for instance, one second of trading interruption equals \$500 million of delayed transactions.

Headline-grabbing risk events are responsible for fewer disruptions to business operations than smaller, more common risk events – such as denial of service attacks and outages due to ISP network failures – and mundane system failures. Gartner, a market researcher, estimates that on average, 40 percent of network downtime is caused by application failures such as performance issues or “bugs,” 40 percent by human error, and 20 percent by system or environmental failures.¹ “Overall, less than 5 percent of application downtime results from actual disasters,” says Professor Uday Karmarkar from the Anderson School of Management at the University of California Los Angeles.

Figures such as these have encouraged the emergence of the new discipline of BCP. BCP's purpose is defined by researchers at George Mason University as “ensuring the uninterrupted provision of operations and services to end-customers.” Whereas disaster recovery is more about specific cure – the restoration of damaged assets, usually after a shattering but unpredictable risk event – BCP shifts the focus to a broader program of prevention – using predictive techniques to identify risks and putting processes in place to ensure continuity of business functions.

¹Aftermath: Business continuity planning, 2001, Vic Wheatman, Donna Scott and Roberta Witty, Gartner, Inc.

BCP: An A to Z

In their research on the travel and leisure sectors, Professors Naresh Malhotra and Saby Mitra of the DuPree College of Management at the Georgia Institute of Technology created a Comprehensive Disaster Recovery/Business Continuity Framework (DRBC Framework) to help companies understand how to go about building an integrated business continuity plan. Utilizing existing frameworks within academic and trade literature, numerous best practices from BCP consultants and case study interviews, the two have identified a sequence of steps to guide firms through the process of BCP planning and ongoing management.

DRBC Framework

Team Chartering	Business Analysis	Define DRBC Strategy	Develop Detailed Plan	Implementation	Maintenance
Secure top-level commitment	Understand business objectives	Define corporate-level DRBC strategy	Define scope of plan	Obtain approvals and buy-in	Set up change management process
Establish a cross-functional DRBC Steering Committee	Identify business outputs, processes and resources	Define process-level DRBC strategy	Document detailed requirements	Develop awareness and education	Monitor performance
Establish DRBC Core Team	Identify DRBC partners and roles	Define resource-level DRBC strategy	Design detailed DRBC Plan	Develop implementation documentation	Keep process up-to-date through performance monitoring, simulations, benchmarking and ensuring that new products, processes and acquisitions are added to the plan
	Identify threats and risks	Define funding and resources		Assign roles and responsibilities	
	Analyze business impacts			Test implementation	

Source: Disaster Recovery and Business Continuity: Travel and Leisure Industry Sector; Naresh Malhotra and Saby Mitra, 2003, DuPree College of Management, Georgia Institute of Technology, Atlanta, Georgia

Leaders and Laggards

While most organizations are aware of the need for business continuity and the majority of companies have some sort of disaster recovery plan, sectors that are more heavily reliant on IT tend to be further along the BCP path.

Take the financial services sector, one of the most progressive industries of all, where outputs, such as certificates of deposits, commercial paper and checking

When comparing industries, the potential revenue loss arising from a network disruption is among the highest for banking and financial institutions.

and savings accounts are, at the most basic level, information products. When comparing industries, the potential revenue loss arising from a network disruption is among the highest for banking and financial institutions.

Typical losses due to network outages		
Industry	Business operation	Average cost/hour of downtime
Financial	Brokerage operations	\$6.5M
Financial	Credit card/ sales authorizations	\$2.6M
Media	Pay-per-view television	\$1.1M
Retail	Home shopping (TV)	\$113,000
Retail	Home catalogue sales	\$90,000
Transportation	Airline reservations	\$89,500

Source: Business Continuity: When disaster strikes, 2000, Fibre Channel Association, Texas

Financial institutions are not alone in being early adopters of BCP, of course. In the U.S., critical infrastructure sectors such as power and water utilities, telecommunications, oil and gas companies and transportation appear to be more generally advanced in the practice. But other industries that have embraced BCP seriously are those whose assets are primarily information, such as R&D-dependent pharmaceutical firms.

At the other end of the spectrum, the retail sector has been slower than other sectors to adopt BCP. The major assets at risk for the retail sector are physical. The largest of these assets are inventories of goods. However, since many firms' inventories are geographically dispersed, the risk of serious loss is greatly reduced. Inventory assets also have the characteristic that they are held temporarily and they have no unique long-term value. In other words, they are replaceable, either in kind or in cash. As a result, traditional insurance works to protect adequately against the monetary impact of losses.

Where BCP has taken hold in retailing, it has again tended to emphasise the IT side of the business. One natural and speciality foods grocery store chain featured in the research is so reliant on the use of networks in the management of inventory that it has created a fully redundant disaster site – a hot spot where several data applications are minutes away from live status – in its own warehouse. The process, managed by a third party, also created workspaces for headquarters employees within their warehouse and included 18 personal computers and telephones to help managers with their continuity efforts. While the warehouse is in a different earthquake zone than their headquarters and data center, the company is currently analyzing how this facility could be moved even further away.

“There is a shift of risk from physical events at the level of stores to the risk of failures in the network infrastructure and information systems that enable e-commerce” — Professor Karmarkar, UCLA

As e-commerce becomes more important to retailers and physical inventories become more centralized, BCP is likely to become more prevalent. One retailer featured in UCLA's research is now realizing 10 percent of its sales from the Internet and its e-commerce volumes equal the sales of 40 of its physical stores. “There is a shift of risk from physical events at the level of stores to the risk of failures in the network infrastructure and information systems that enable e-commerce,” concludes Professor Karmarkar.

Beyond IT

The focus on information technology is not surprising, but risks to business continuity are not restricted to network failures and lost data. One significant threat to business continuity identified in the Michigan State University research comes from sole suppliers. When only one supplier is available to a firm, either through a monopoly on the market or a conscious decision on the part of the buyer, it becomes absolutely critical for the buying firm to validate its partners' BCP practices and independently develop profiles of high-risk suppliers. More critical still are Service Level Agreements (SLAs) that define recovery time objectives if the product or service is critical to the success of the buying firm.

Supplier risk profiles are used to identify those suppliers that should be monitored on an ongoing basis through the use of predictive metrics such as financial reporting. In one example pointed out by the Michigan researchers, a firm identified a supplier as high risk after the supplier offered steep discounts in exchange for immediate payments that would have otherwise occurred over a period of three months. The firm then regularly reviewed analyst ratings and other tools to monitor the health of the supplier company and thus better assure the continued flow of incoming goods and services.

Best Practices: Be Prepared

The research reveals that while almost all organizations are aware of the need for business continuity and the majority of companies have some sort of disaster recovery plan, most companies need to rethink what it means to ensure continuous business operations. The true pioneers in the field of BCP exhibit the following attributes:

They do more than concentrate on tangible assets such as systems, networks and physical assets. Effective BCP isn't simply a matter of keeping critical data in more than one location or building redundant systems; it addresses equally important aspects of organizational discontinuity such as employee education, alternative work processes and communication with customers. Training is a critical element in any BCP plan.

They learn from their mistakes. The Michigan researchers observed that when supply chain disruptions occurred, for instance, the best firms learned from them. "A serious disruption requires a post-incident audit that identifies important lessons learned-things that went right and things that went wrong," says Dr. Zsidisin. But even within the company that was most advanced in the use of audits, the process was managed by the buying organization, not the supply chain partner where the actual disruption occurred. Unless the suppliers take responsibility for the audit's execution, an audit has limited utility as a tool for self-improvement.

They are open to using third-party providers. Outsourcing BCP functions to third party providers that store critical company data and make available alternative facilities to continue such operations in the event of a disruptions can provide significant protection, particularly when IT processes are not a firm's core capability. Using managed service providers can also enable companies to keep pace with rapidly changing IT environments and continuity needs.

BCP is integrated across firms. The increase in complex interactions among applications across an organization and its partners means that disruptions at one point may propagate rapidly throughout an organization in ways that may not be easily and quickly understood. Rather than asking business units to handle BCP within their own

silos, an integrated approach is needed. That doesn't just mean handing the job to the IT department – functions such as human resources and customer service need to be in the loop.

Plans are tested and updated on a regular basis. Companies with untested plans may face as much risk as those with no plans at all. Where testing was observed in the universities' research, it was often limited to the evaluation of system or data backup and restoration and not the actual restoration of business functions. The research identified cost concerns as the major impediment to regular and comprehensive testing, but saving money in this way is a false economy – an outdated or ineffective BCP program has next to no value.

Above all, BCP is perceived as more than a cost. Despite their relatively advanced BCP programs, even executives in the financial services industry see BCP primarily as merely a cost of doing business, a kind of insurance. “BCP was not seen as value-added activity that might be used to garner competitive advantage in any of our case studies,” says Amitava Dutta, professor of Management Information Services in the School of Management at George Mason University.

That is shortsighted. Business customers, particularly in industries such as financial services, where speed, privacy and security are at a premium, are beginning to ask questions about emergency preparedness. Being able to demonstrate developed BCP programs can be a source of reassurance and a positive element of brand positioning. Shareholders place increasing weight on effective risk management, of which BCP is one element. Companies themselves can turn the flexibility and resilience implicit in BCP to their advantage by being able to ramp up production levels or divert supply chains in response to spikes in demand. BCP is designed to cope with failure, but it can also help to ensure success.

BCP is designed to cope with failure, but it can also help to ensure success.

Business Continuity Planning research papers funded by the AT&T Foundation:

Business Continuity in Financial Services: Perceptions of Senior Management, Amitava Dutta, Mahesh Joshi and Linda Parsons, 2003, School of Management at George Mason University, Fairfax, Virginia

Business Continuity Planning in the Pharmaceutical Industry: Assessment Model, Paul Rohmeyer and Edward Stohr, 2003, Howe School of Technology Management, Stevens Institute of Technology, Hoboken, New Jersey

Business Continuity and Technology in the Retail Sector, Uday Karmarkar and Vandana Mangal, 2003, The Center for Management in the Information Economy (CMIE), the Anderson School of Management at the University of California Los Angeles, Los Angeles, California

Disaster Recovery and Business Continuity: Travel and Leisure Industry Sector, Naresh Malhotra and Saby Mitra, 2003, DuPree College of Management, Georgia Institute of Technology, Atlanta, Georgia

Effective Practices in Business Continuity Planning for Purchasing and Supply Management, George Zsidosin, Gary Ragatz, and Steve Melnyk, 2003, Department of Marketing and Supply Chain Management, The Eli Broad Graduate School of Management, Michigan State University, East Lansing, Michigan

About AT&T

For more than 125 years, AT&T (NYSE "T") has been known for unparalleled quality and reliability in communications. Backed by the research and development capabilities of AT&T Labs, the company is a global leader in local, long-distance, Internet and transaction-based voice and data services.

About the AT&T Foundation

The AT&T Foundation invests in education, arts and culture and community service projects that serve the needs of people in communities throughout the nation, particularly for initiatives that use technology in innovative ways and for programs in which AT&T employees are actively involved as contributors or volunteers.

About The Economist Intelligence Unit:

The Economist Intelligence Unit is the business information arm of The Economist Group, publisher of *The Economist*. Through its global network of over 500 analysts, the Economist Intelligence Unit continuously assesses and forecasts political, economic and business conditions in nearly 200 countries. As the world's leading provider of country intelligence, the Economist Intelligence Unit helps executives make better business decisions by providing timely, reliable and impartial analysis on worldwide market trends and business strategies. (www.eiu.com)

For more information, contact your AT&T
Representative, or visit www.att.com/business.



AT&T

The world's networking companySM