Business Continuity and Technology in the Retail Sector

Uday S. Karmarkar

Vandana Mangal

February 2, 2004

The Business and Information Technologies Research Project

The Center for Management in the Information Economy

The Anderson School of Management at UCLA

Abstract

This study examines business continuity in the retail sector. Business continuity can be defined as contingency planning undertaken to ensure the best possible continuance of business activities of a firm in the event of unforeseen events (such as natural disasters) which interrupt the normal functioning of the firm.

The study consisted of four major parts:

- A mail survey of business continuity practice in retail firms
- Case studies of business continuity practice in selected firms
- Secondary research using library and web sources
- The development of an economic framework for business continuity in retailing

Based on research, surveys and case studies, the study found that retail organizations are aware of the need for business continuity. However, although most organizations have some sort of disaster recovery plan, they tend to emphasize the information technology issues, while other aspects of the organization such as employees and physical structures are not always included. Even among the organizations that have business continuity plans, the plans are not tested and updated on a regular basis. Among the factors cited as the reasons for the lack of well-developed business continuity plans, cost is the major issue.

The events of Sept 11 have not had a major impact on business continuity planning in retail organizations. There may have been a short period when organizations paid greater attention to business continuity. However, that spike has now disappeared. This may be due to the fact that although disasters such as the events of Sept 11 are given great importance in the media, 95% of the downtimes in organizations (retail or otherwise) are caused by local factors and events that are not totally unforeseen. These factors include floods, fires, viruses, disaffected employees, theft, and power or telecommunication failures.

Retail organizations display certain characteristic features that appear to diminish the incentives for continuity planning. The assets of retailing firms are primarily in the form of inventories, which tend to be geographically dispersed. This provides automatic protection against many kinds of disruptive events. Since the inventories are part of a flow of sales, they do not have long-term asset value. In other words, they are replaceable. Inventories are typically covered by insurance, which adequately protects retail organizations against the monetary impact of losses. The retail sector has not seen many new developments in the management of these assets. This is partly because recent events such as the terrorist attack of September 11 are not seen as having created any new kinds of risks for retail. However, this may be a somewhat myopic view; were there a disruption of say port facilities due to terrorism, then there would be an impact on the flow of goods, which would be quite significant.

Retail organizations also have some informational assets. The preferred mode of managing informational assets has shifted from paper to telecommunications technologies. As a result, with better telecommunications technologies and lower storage costs, the risk to informational assets has reduced. It has become easier to maintain distributed databases using network resources, which are inherently more robust. As a result, many firms simply need to put into place, alternative sites for accessing these resources. Of course, telecommunications infrastructure downtime, remains as a risk factor.

Table of Contents

Business Continuity and Technology in the Retail Sector

Uday S. Karmarkar
Vandana Mangal
Business and Information Technologies (BIT)
The Center for Management in the Information Economy (CMIE)
The Anderson School of Management at UCLA

Acknowledgements

The authors of this report would like to thank AT&T for their support to conduct this study.

Introduction to Business Continuity and Business Continuity Planning

Business continuity (sometimes referred to as *business continuance*) describes the processes and procedures an organization puts in place to ensure that essential functions can continue during and after a disaster [1]. This paper focuses on business continuity in businesses with emphasis on technology and the retail sector.

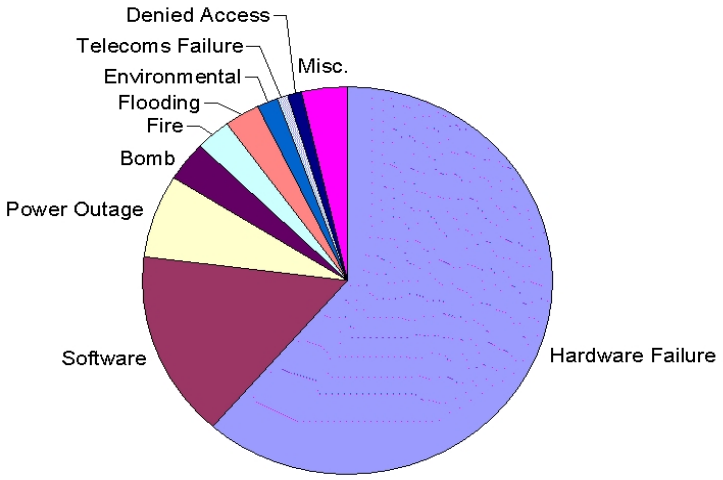
Disasters can be caused by any of the following:

- ***Natural causes*** such as floods, fires and earthquakes
- ***System related causes*** such as network problems, power and telecommunication failures or,
- ***Human and Malicious causes*** such as hackers, viruses, terrorism, disaffected employees and theft

Most people think in terms of fire, flood or some other cataclysmic events when they consider risks from disasters [9]. In reality, it is the small events (rather than catastrophic disasters) that have a higher likelihood of interrupting normal business operations. Some recent examples of disasters are listed below:

- The 3-day Microsoft Web site outage disaster in January 2001
- Denial-of-service attacks on various organizations at various times
- Limited capacity causing spikes in business volumes due to a fashion show event as in the case of Victoria's Secret Retailer
- Application failure as with the London Stock Exchange outage in April 2000
- Partner/outsourcer unavailability such as ISP network failure
- Loss of physical structures such as those due to fire at the Los Alamos National Laboratory

The above is supported by a report from [9], which states that, on average, 40 percent of downtime is caused by application failures such as performance issues or "bugs," 40 percent by operator error, and approximately 20 percent by system or environmental failures. About 60 percent of these system or environmental failures are caused by hardware problems. Overall, less than 5 percent of application downtimes result from major disasters.



The question then is why this 5 percent of downtime garners so much attention. A survey conducted by Information Week Research on downtime and business continuity in organizations reports that 25% of the participating organizations had to invoke their business continuity plans in the last year, with 70% reporting the disaster as severe or extremely severe. Therefore, in spite of cataclysmic disasters contributing to only 5% of downtime in organizations, being prepared for disasters and having a business continuity plan are essential for all business organizations.

In today's web-oriented business world, organizations need to be concerned with the risk of downtime. Any downtime in an organization will result in negative media coverage in addition to loss of large sums of money, which can impact a company's image, loss of customer confidence and in some extreme cases, the company's very existence. Losses due to downtime to businesses in some sectors are listed in the table below [9]. These numbers do not take into account effects such as the impact to company reputation and loss of customer confidence.

Industry	Business Operation	Average cost/hour of downtime
Financial	Brokerage operations	$6.5 million
Financial	Credit card/sales authorization	$2.6 million
Media	Pay-per-view television	$1.1 million
Retail	Home shopping (TV)	$113,000
Retail	Home catalog sales	$90,000
Transportation	Airline Reservations	$89,500

Given the huge losses that a business can incur due to just 1 hour of downtime, it is critical for today's businesses to plan and prepare for business continuity in the event of a disaster. Should

organizations develop Business Continuity Plans to be prepared for disasters? Are businesses investing in Business Continuity or was it only a spike after the terrorist attacks of September 11, 2001 in the United States? These are some of the questions this paper aims to address.

Business Continuity Planning (BCP) is described in detail in the following section.

Business Continuity Planning (BCP)

Business Continuity Planning (BCP) seeks to prevent the interruption of mission-critical services, and to reestablish full functioning as swiftly and smoothly as possible [2]. Business Continuity Planning in the early 1990s was focused primarily on ***disaster recovery***. Disaster recovery deals primarily with information technology systems and applications. In the event of a major disaster, networks, applications, systems and data had to be recovered at another location. The typical recovery time objective (RTO - the desired time to recover applications) was approximately three days; the typical recovery point objective (RPO - the acceptable transaction loss) was 24 hours. Most organizations that implemented disaster recovery plans did so because they were in highly regulated industries such as financial services, government, health and regulated utilities.

BCP gathered momentum in the late 1990s, partly due to preparation for the Y2K crisis. Many businesses began to understand that if their systems and applications failed, their business processes would fail along with them, thereby impacting their bottom line. This provided the needed incentive for organizations to begin investing in BCP and disaster recovery between 1997 and 2000. RTOs for mission-critical business processes were reduced to as little as 24 hours and RPOs were often set to the point where there would be zero transactions lost.

The growing interdependencies among organizations' internal systems and their contractors' systems began to increase the complexity of recovery in the event of a disaster. In addition, the advent of the Internet and e-business in 1999 changed the way businesses thought about BCP. Businesses began integrating their business processes with those of their customers, suppliers and business partners resulting in further reduction of RTOs and RPOs for mission critical applications

Business Continuity awareness has increased tremendously since the terrorist attacks of September 11, 2001 in the United States. This caused an increase in disaster recovery and business continuity budgets immediately following the event. Many organizations have assigned dedicated business continuity coordinators or directors and have involved high-level non-IT decision makers in BCP. In a survey conducted for Information Week Research of 250 IT and business managers responsible for business continuity planning, Price Waterhouse and Coopers found that over half the managers reported that their organizations are likely to increase BCP spending. According to Meta Group [2], high-end BCP budget numbers are expected to approach to 5% of IT budgets by 2005.

However, in spite of increased in BCP awareness since 9/11, studies report that two-thirds of the 1000's of businesses they surveyed did not have business continuity plans and even among the businesses that did, four-fifths had never tested their plans. Of the companies that had tested their plans, only 17% of the plans had passed.

What does BCP involve?

Although companies may follow different processes for BCP, most businesses typically use the following methodology [3]. The table shows that business continuity planning is a 3-step process that includes analysis, plan execution and plan maintenance. BIA is the most important step

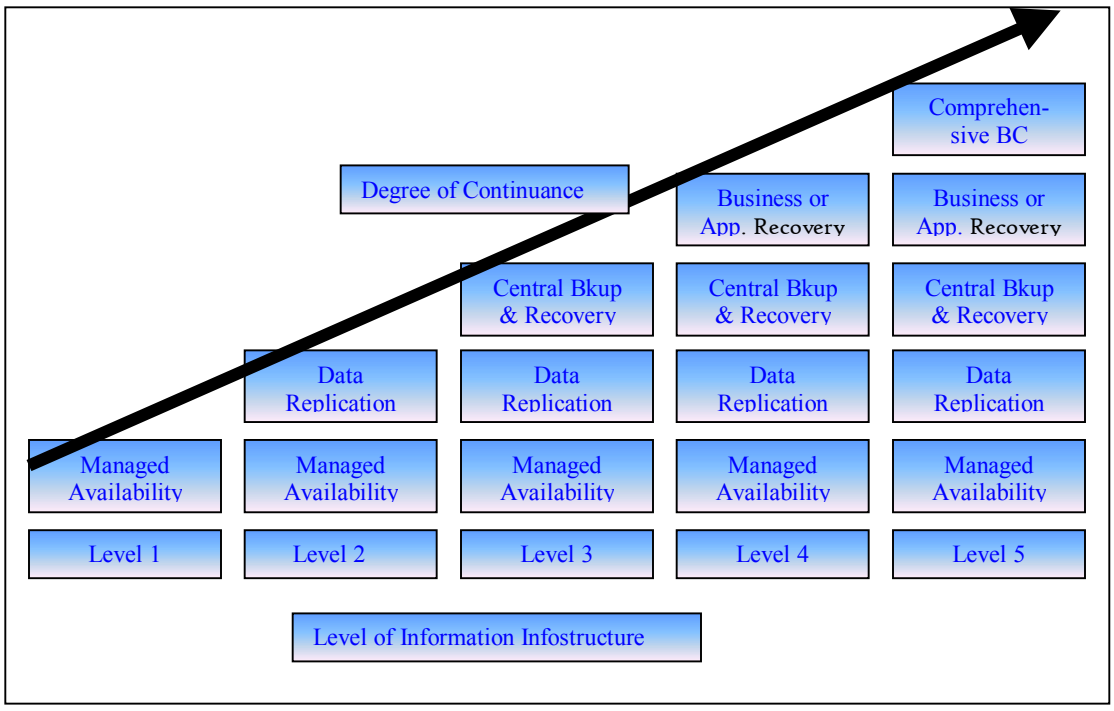
during analysis. BCP may be done in-house, by working with consultants who specialize in BCP initially and later managing the plan in-house or by contracting the entire process to an external entity.

Step 1	**Developing the Foundation**
Audit Analysis	Identification of the enterprise's assets, which will include, but not be limited to, people, facilities, business applications, processes, and IT systems (hardware, software, files, and communications)
Risk Analysis	Identification of the threats, mitigating factors, and dependencies, including the definition of the types and scope of disruptive events
Business Impact Analysis (BIA)	Measure of the operating, financial, legal, and regulatory impacts of a disruption to an enterprise's operation--identification of the critical business functions and the costs of downtime for each asset. Definition of RPO and RTO objectives for each asset and the prioritization of assets into defined categories, such as critical, vital, sensitive, and non-critical
Step 2	**Developing the Plan**
Funding Approval	Commitment and financial approval from senior management
Review Existing Plans	Incorporation and adoption of proven best practices within the enterprise
Recovery Strategy	Definition of the continuity model, tasks, processes, technology, roles, and resources required to meet stated RPO and RTO objectives and prioritization levels--forming the plans for disaster recovery, business resumption, business recovery, and contingency
Step 3	**Maintaining the Plan**
Training	Creation of awareness and knowledge of the plan
Testing	Continuous testing against the plan, review of results, and modification appropriately
Keeping Informed	Update of plan to reflect changes in the enterprise's assets or operational, financial, legal or regulatory environment

Business Continuity includes people, assets, financial liabilities, change management and technology. This paper will focus primarily on technology in business continuity. This is discussed in the following sections.

Technology in Business Continuity

Although business continuity is important for any business, it may be practical only for the largest organizations to maintain a full functioning plan throughout a disaster crisis. For all other organizations, the first step in business continuity planning should be deciding which of the organization's functions are essential, and assigning the available budget for these functions accordingly.



The level of information that will be available after a disaster will be proportional to the degree of continuance an organization has planned for. As shown in the chart, the degree of continuance is lowest at Level 1 and highest at Level 5. Several alternatives are available for recovery of data and applications (information) in the event of a disaster. These are discussed in the next section.

Recovery Alternatives

Recovery alternatives are listed below [6]. Off-site data storage is the most basic solution, which is used by most organizations today. Cold and Hot sites are also maintained by several organizations today, although these are more expensive to develop and maintain.

- **Off-site Data Storage**: Storage on tape or disk to a different physical location. Depending on budget and geographical risks, off-site storage could be the building next door, a bank safety deposit box, or the branch office across town. A better choice is a secure, climate-controlled, fireproof media vault at a storage facility maintained by a commercial media storage provider.

- **Disk-to-disk Remote Copy**: Operates at the disk volume level and is significantly less complex to set up and administer than host-based replication. This is the most popular solution used today. The solution benefits from capturing all application environment changes. A drawback however is the lack of transaction knowledge and the potential for data corruption in the event of a disaster. Most disk-to-disk remote copy solutions operate in synchronous mode, which degrades performance of production applications unless the solution can be deployed over fiber link to the recovery site. The distance can generally be from a few kilometers up to about 60 km

- **Cold Site**: Empty, environmentally conditioned computer room with office space, telephone jacks, etc. ready for the computer equipment to be moved in. The cold site is available on a

subscription basis, much more cheaply than a hot site, but because the customer provides and installs all the equipment needed to continue operations, it takes longer to get an enterprise in full operation after the disaster. Often such equipment is provided through a contract with an equipment leasing company

- **Hot Site**: Fully equipped, operationally ready data center offering specific hardware platforms ready for almost immediate use when the service provider is notified of a disaster. A hot site has all the equipment needed for the enterprise to continue operation, including office space and furniture, telephone jacks, and computer equipment. Employees report to work at the hot site instead of the usual location. Subscriptions to commercial hot sites are based on the hardware specifications and generally allow hot-site use for up to 8 weeks in disaster mode

- **Electronic Vaulting** (or Advanced recovery services): Data sent directly from the subscriber site to the hot site. This costly service requires that a direct-access storage device (DASD) be dedicated to the subscriber, preventing the service from being shared with other subscribers. PC/LAN electronic data vaulting is emerging as a popular service

- **Shadowing**: Maintains a replica of the database and/or file systems, typically by continuously capturing changes and applying them to the recovery site. Shadowing is an asynchronous process, thus requiring less network bandwidth than synchronous mirroring. The RTO is relatively small, typically 1 to 8 hours, while the RPO is as up-to-date as the last receipt

- **Mirroring**: Maintains a replica of databases and/or file systems by applying changes at the secondary site in lock step with or synchronous to changes at the primary site. Due to its synchronous nature, mirroring requires significantly greater network bandwidth than shadowing. The RTO is around 20 minutes to several hours, while the RPO is reduced to the loss of uncommitted work

The above recovery solutions can be provided by any of the major BCP players in the market today. Major players are listed in the next section.

Major Players in BCP

Today, the major players in Business Continuity Planning are [9]:

- IBM [4]

- HP [5]

- Comdisco, now purchased by Sunguard [6]

In addition to providing complete solutions, some of them such as IBM also provide consulting services. Several consulting companies that specialize in Business Continuity Planning also exist. Solutions are offered in various sectors. The next section focuses on Retail.

Business Continuity in the Retail Sector

The Retail industry has traditionally been slower to adopt business continuity planning. This has been in spite of point-of-purchase vulnerabilities prevalent throughout their processes and flow of information in the supply chain. Costs have been considered the biggest barrier to the slow acceptance BCP in retail. Retail is a business that is mission critical and its applications need to be available 24x7. Retailers also cannot afford to lose any data.

The supply chain for retail has several points (from store to distribution to Head Quarters) at which disasters can occur. Some of these points include [7]:

- Credit and debit card systems function so not alienate customers
- Digital signatures
- Bar code scanning (pricing errors, customer dissatisfaction, customer alienation)
- Ordering
- Receiving
- Moving to shop floor
- Paperless and wireless warehouse
- Dispatch

In retail, downtime can cause an organization as much loss as $100,000/hour [9].

Research Methodology

To understand Business Continuity initiatives and practices in retail organizations, a survey is being conducted. Each subject in the study is an independent organizational entity, which controls its own information technology and information policy, and has a CIO or similar management position within it. It is highly likely that since the subject organization is able to make its own technology decisions (and investments) that it will have profit and loss responsibility, although this is not necessarily always the case. The surveys have been addressed to the CIO (or similar position) as the person most likely to be knowledgeable about the subject.

The following steps have been followed in the compilation of the survey:

- Issues relevant to business continuity in retail have been identified. Some of these issues as whether organizations have business continuity plans, who implements them, who leads their execution, how they are communicated to the employees and who other than the internal organization is included in the plans
- A business continuity questionnaire has been compiled based on these issues.
- A database containing the names and contact information for the relevant officers in retail organizations has been procured. The database contains names and contact information for CIO and similar officers in the retail sector for 2000 organizations
- A package with the questionnaire and a cover letter explaining the study has been mailed to the retail organizations in the United States and Canada

The survey can be taken on paper or online. An online version of the questionnaire has been developed using a survey tool called Zoomerang. The online version is available at http://www.anderson.ucla.edu/research/bit.

In addition to surveys, a limited number of case studies have been conducted to obtain an in-depth understanding of the issues in retail. Executives and Managers who head the major divisions in their organization have been interviewed. Focus has been on understanding the critical processes in these retail organizations and on business continuity.

An Economic Framework for Business Continuity Planning

Business continuity planning (BCP) can be framed in terms of a decision making process that trades off the potential cost and risk of unforeseen events against the costs of protecting against the consequences of those events. In this sense, BCP is analogous to other forms of risk management including insurance, hedging, or planning against random failures. The frameworks, models, and techniques that are used in these well-developed areas (risk analysis, failure trees and event analysis, reliability methods, insurance, financial risk management) are all applicable to varying degrees. Here we will not survey all these methodologies and their potential applications. Rather we outline the major characteristics of BCP, and also consider some of the special aspects of BCP in the retailing sector.

The elements of the problem include, the causative events, the consequences or outcomes, and the losses that are associated with these outcomes for the business. In general, while the causative events can be of many types, they are all characterized by low probability of occurrence in any given time period, and randomness with respect to the time when the event will occur. Forecasting these events first requires estimating the distribution of time till the next occurrence of each event. Since the events are random low probability occurrences, an exponential distribution is likely to suffice for most cases. The complementary information that is required is the cost impact of each event, which may also be a random variable. A typical model for the magnitude of the loss would be a distribution such as the log-normal, reflecting the nature of losses, which are likely to be heavily skewed. Based on these, the expected present value of the costs due to the causative events can be estimated, along with the risk (e.g. the variance of costs incurred or other measure of risk).

The next part of BCP analysis would be to list all the protective measures that can be taken with respect to each category of outcome. These measures can include a large variety of possible actions directed towards each kind of event, including approaches for the minimization of costs, and working towards recovery from the event.

This is a very general model. The analytical methods involved are well known from the disciplines mentioned earlier. Applying it is a lengthy process because of the large number and variety of causative events that might be relevant, and the number and complexity of different outcomes, consequences and costs, which may all be uncertain. Here we do not go into the technical details of modeling events, consequences, the efficacy of different activities, or the choice problem of which activities to implement. Rather we describe the characteristics of the planning issues for companies in the retail sector.

The losses related to outcomes can be broadly classified into the categories of

- lost assets (physical, information)
- lost productive time and lost revenues due to the breakdown of systems, or due to damage or danger at retail sites
- lost goodwill or lost customers, due to a period in which customers experience either direct costs, or perhaps simply a lack of access to goods and services

For the retailing sector, the major assets at risk are physical. The large part of these is inventories of goods in transportation pipelines, in storage (warehouses) or at retail locations. For many firms, the inventories tend to be geographically dispersed. As a result, the risk of loss is greatly reduced through diversification since the causative events (disasters, attacks) are usually geographically localized. Of course, there are some events that can affect all inventory sites (as

for example a national crisis such as a war) but such an eventuality could be considered to lie outside the scope of BCP.

The inventory assets also have the characteristic that they are part of the flow of goods through the company. The implication is that the assets 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 cover company risks.

Retail companies do not tend to have large information assets (unlike say financial services companies, or media companies). However we note that modern information technologies have resulted in a shift of information storage and processing from paper to electronic form. From a BCP perspective, the result is a centralization of information and information processing assets. However, the same modern technologies also make it very simple to protect against excessive decentralization, through a number of means, including simple duplication of data and systems.

The next major category of risk is that of lost productive time. Over a short term period, the major operating concerns in retailing (apart from immediate disaster management) have to do with information flows between vendors, inventory and logistics systems, and retail locations, which in turn have value because they relate to physical flows and financial commitments (invoices, purchasing documents, orders). Here information technologies permit a decoupling between physical working space for staff, and the information systems required. So (as illustrated in one case study) all that is necessary to provide a back up working environment is a set of workstations, that can be connected through telecommunications, to the relevant information systems.

The issue of lost retailing time, and temporary loss of access by customers, is a physical issue. For retailers, geographical dispersion is again a saving grace that reduces risks. There are clearly a number of systems and procedures that are required at each retail store location. However, for the most part, the kinds of threats and disruptions that affect these sites are not new to the industry. As a result, we do not see any major change in practice from traditional approaches.

In the future, it is likely that there will be some shift in retailing from bricks and mortar to web based sales. As this shift occurs, there will be a corresponding centralization of systems, and a concentration of risk in the direction of web sites, and the internet infrastructure. Physical inventories will also become more centralized. As an example, one of our retailers, now sees about 10% of it's sales occurring on the web, which corresponds to about 40 or so physical stores. Overall, this is really a reduction in the magnitude of risk in terms of physical assets, since the increased risk in centralized inventories is offset by the benefits of pooling inventories. There is also a shift of risk from physical events at the level of stores and storage facilities, to the risk of failure of the telecommunications infrastructure and information systems. However, protecting against problems in these systems is much simpler and well organized. In many cases, third party service providers already have many safeguards in place.

In future research we will be developing a formal model of continuity planning and risk management that can be applied to any industry, to determine the best approaches to BCP for a given company in a given sector.

Summary of Survey and Case Results

Some survey responses have been obtained; additional responses are awaited. Complete results will then be compiled.

Compilation of the current responses to the survey brings forth some interesting results. These are listed below:

- 45% of the respondents currently have a business continuity plan; 30% are developing plans; 25% will develop plans. None of the respondents do not intend to develop any plans
- Emails, group meetings and corporate presentations are the most popular methods of communicating business continuity plans to the employees. Written documentation as in binders is also used by almost 20% of the respondents for communication of plans
- Most respondents develop the requirements for business continuity and network/IT security needs in-house with some of the respondents developing them with the help of a third party
- CIO's or CFO's generally oversee the business continuity planning process. Business Continuity plans are generally implemented by the CIO or the IT Director/Manager
- Phones/Cell phones/pagers are listed as the most popular method of communicating with employees in the event of a disaster followed by email
- Although most organizations review their plans and conduct recovery exercises annually, several respondents have never tested their plans and do not plan to test them in the future
- Among various technology options for disaster recovery, almost all of the respondents have offsite data storage; the numbers for other technology options are not as high although some of the respondents have mirroring
- About a third of the respondents involve their IT departments in business continuity recovery. Interestingly, 20% include internal business organizations and 24% include vendors. However, only 12% include suppliers, and 10% include contractors. None of the respondents use offshore contractors for business continuity recovery
- Most respondents use workplace assessment as the risk assessment method (38.2%) followed closely by quantitative risk assessment (35.3%)

Review of case studies in retail has shown that although most organizations agree that business continuity is important, businesses have not allocated large budgets for it. The only aspect of business continuity that has been prepared for in organizations is technology and data retrieval. The most popular method used is offsite backups. Most organizations also have cold sites and some also have hot sites. The executives of the three companies discussed in the mini cases the Appendix felt that they were reasonably prepared for a disaster and would be able to have their operations up and running within a short period of time. Two of the three corporations have also been planning to set up backup data warehouses and data centers in different time zones to ensure business continuity in case of a catastrophe. In general, retail companies are somewhat protected in the event of a disaster due to their stores being geographically distributed. The main warehouse is the main concern in terms of physical assets.

Conclusions

The main conclusions from the survey, case studies and economic framework, are:

(i) The assets of retailing firms are primarily in the form of inventories

(ii) These assets (inventories) tend to be geographically dispersed which provides automatic protection against many kinds of disruptive events

(iii) Since the inventories are part of a flow of sales, they do not have long term asset value. In other words, they are replaceable.

(iv) Inventories are typically covered by insurance, which protects adequately against the monetary impact of losses.

(v) The retail sector has not seen many new developments in the management of these assets. This is partly because recent events such as the terrorist attack of September 11 are not seen as having created any new kinds of risks for retail. However, this may be a

somewhat myopic view; were there a disruption of say port facilities due to terrorism, then there would be an impact on the flow of goods, which would be quite significant.

(vi) Retail organizations also have some informational assets. The preferred mode of managing informational assets has shifted from paper to telecommunications technologies. With better telecommunications technologies and lower storage costs, the risk to informational assets has reduced.

(vii) The events of Sept 11 have not had a major impact on business continuity planning in organizations. There may have been a short period when organizations paid greater attention to business continuity. However, that spike has now disappeared

(viii) Although disasters such as September 11 are given great importance in the media, 95% of downtimes in organizations (retail or otherwise) are caused by local factors and events that are not unforeseen. These factors include floods, fires, viruses, disaffected employees, theft, and telecommunication failures.

(ix) Organizations are aware of the need for business continuity. However, although most organizations have some sort of disaster recovery plans, they tend to emphasize the information technology side, other aspects of the organization such as employees and physical structures are not always included.

(x) Even among the organizations that have business continuity plans, the plans are not tested and updated on a regular basis.

(xi) Among the factors cited as the reasons for the lack of well-developed business continuity plans, cost is the major issue.

References

[1] http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci801381,00.html

[2]http://www.acmsyr.org/Meetings/Meeting%20Materials%202002/Program_02_10.pdf

[3] http://www.equant.com/content/xml/connectonline_june_business_continuity.xml

[4] http://gartner.library.ucla.edu/research/90800/90811/90811.html

[5] http://www.hp.com/hps/tech/continuity/

[6] http://www.availability.sungard.com/Products+And+Services/Business+Continuity/

[7] http://www.emc.com/pdf/vertical/retail_bc_dr.pdf

[8] http://gartner.library.ucla.edu/research/95100/95187/95187.html

[9] Gartner Group reports

Appendix: Mini Cases

Two case studies have been conducted. The first is for a teen clothing and accessory retail chain. This is called Company A for the purpose of this report. The second company called Company B in this report is a specialty grocery store chain.

Company A:

Company A is a clothing and accessory retailer for male and female teens. It is a growing company. It started as one store in one mall. The company now has almost 500 stores across the United States. In the fifteen years since Company A was started, their revenues have grown from under $1 million to $443 million.

The clothing retailer distinguishes themselves from other teen fashion stores by keeping music as the focal point of their merchandise. Over the years, styles have taken an alternative focus, covering genres like gothic, metal and punk rock, mirroring the tastes of Company A's customer base. Styles are based on the latest bands and their music.

Company A has realized that their customers can help them determine trends. They use several different methods to obtain information from their teen customers. These are listed below:

- report cards are available in all their stores for customers to fill out
- store employees are encouraged to call in with trends they observe or hearing about from their customers
- a "Mouth Off" section on their website sends feedback directly to the relevant department in the company
- company buyers ensure they are everywhere the music is, including concerts to see and hear teenagers and bands clothing and accessories

In addition to their regular store, Company A also has an internet store which is equivalent to 16 mall stores in terms of the volume they handle. Online, Company A has tried to recreate the community feeling by adding additional features to their site including: streaming music, band reviews, upcoming musical events, polls and a feedback/chat forum called the Mouth Off section. The website is also used for marketing. Registered users receive emails of upcoming events as well as new themes and products. The underlying technology is performed entirely in-house including web hosting.

Company A has recently contracted their business continuity planning to a consulting firm. The firm is responsible for putting the systems and processes in place to keep the company running in the event of a natural or man-made catastrophe. This includes communication to and from stores, the distribution network, the electronic network and all other home office functions. Currently, the electronic network is the only segment of the business with any notable contingency planning, having redundant database storage although no offsite redundant web servers. The data center also currently lacks redundant load balancers or routers for the Internet operation. This means that if customer traffic significantly increased or servers went down, Company A could temporarily not take orders from customers online. Onsite, motor generators have been installed for the data center which is protected by FM200 fire suppression and an internal air conditioning unit. However, if an event prevented access to the home office, and therefore DC and data center, merchandise orders cannot be processed and products cannot be shipped out.

The scope of their business continuity plan will encompass their headquarters and warehouse/distribution center. A program will also be rolled out to the retail stores throughout the country. The company plans is to determine the risks to the company and to develop a plan that will cover people, technology, warehouse and their computer systems in the event of a disaster. Their plan is to keep all these procedures documented in a manual. This manual will also identify recovery team members, call lists, resources and additional information needed for a successful recovery. Restoration and salvage considerations will also be included.

A crisis communication program to deal with the press and to communicate with employees and their families, key customers, critical suppliers, corporate management and owners/stakeholders is also planned. They also have plans to train staff on the contingency procedures and responsibilities during a disaster for business continuance. Although IT is involved in the business continuity planning process, a special coordinator has been assigned for this purpose.

In summary, Company A has realized the need for business continuity planning. They are working with a consulting group to put together their business continuity plans and have plans of developing a complete company wide business continuity plan.

Company B:

The second case study is for a "natural and specialty foods" grocery store chain. Company B started over 45 years ago as a chain of convenience stores in Southern California. About 10 years later, to enhance their image, they started carrying boutique wines and gourmet foods at exceptional prices. Now they have almost 200 stores in 17 states in the United States. Company has been able to develop a large customer base through reputation alone. The retailer targets young, educated buyers by focusing on what is important to them such as natural and organic foods.

Their mission still remains the same – to bring the exceptional wines and fresh, minimally processed foods and beverages to their customers at outstanding prices. They therefore do not compete directly with other grocery chains and have been able to carve a niche for themselves. Due to their unique business model, they are often called "store of stores".

They are able to accomplish the above business model by buying directly from suppliers whenever possible hence are able to avoid middleman costs and negotiate better with their suppliers. They buy their products in large quantities. They pay their suppliers in cash and on time so people like doing business with them. All their products are sold under their own brand. A product that is unable to pay its own way is discontinued. They also manage their packaging, distribution and advertising costs in-house. Advertising is minimal – it is done primarily by a radio spot they have or by their magazine which is available online (mailing it out for getting too expensive). All of these allow them to keep their costs low and hence prices of their products low.

They keep their customers coming back by introducing 10-15 new products each week. Taste tests are conducted before any new product is introduced.

Although they have grown to 7488 employees (as of 2001), they still maintain a small company culture that is very casual. Hawaiian shirts are the norm there from employees at the stores to the CEO himself.

Company B has a web presence. However, it does not have sell products by mail order or using e-commerce at this time. Their website is to provide "information" and serves the following purposes:

- educate and inform customers on their products
- advertise and market their brand
- recruit new employees

Their stores average about 10,000 sq. ft and they carry over 2000 private-label products.
Company B is a privately held company and is very "private". Hence it is difficult to get their numbers. Hoover's estimates their annual sales at $1,900 million in 2001 and their 1-year sales growth is 13.8%.

Business Continuity is viewed as a serious issue for Company B, more on the technology front. They have a fully redundant disaster site – a hot site where several applications are minutes away from live – in their own warehouse. It is a "lights-out" facility. Some critical applications are also shadowed. Other applications are backed to tape and kept in a vault off-site. This process is managed by a third party. These applications would be up and running in 12 hours. Their warehouse is 35 miles from their headquarters. It is on a different earthquake fault than their headquarters. They are currently analyzing how they can have this facility further away than it currently is, perhaps in a different state.

As part of their Business Continuity planning, Company B has performed Business Impact Analysis (BIA) which has included going through various scenarios from not being able to get into their headquarters building even though the building and equipment are fully functional to if the building is destroyed. This has also included identifying the criticality of their applications and assigning RTOs and RPOs based on it. The RTO for critical applications is under 5 minutes. The systems for buyers is updated every 15 minutes? In addition to setting up the hot site facility for their systems, they have also created some extra space in the warehouse that can house 18 PCs and phones, etc. This would not be sufficient to accommodate everyone in the event of a disaster. However, it would allow the business to get started and up and running. They also have a facility that houses 30 employees in the Boston area where they will also be creating a backup site. Currently, the company has a server farm where there are redundant systems. All 200 stores are linked through the remote site as well as this site.

Their computer systems include primarily internal applications such as HR, payroll, etc. Merchandising (inventory and warehouse) is their most critical applications. They have an internet presence which is primarily informational. The development, maintenance and hosting of the website is currently outsourced. They also have a backup facility. They have been reviewing the idea of bringing it in-house.

Their primarily IT oriented BC plans has been extended to take care of employees by using what they call a "red book". All IT employees carry it at all times. It contains the current phone book, vendor contacts and key employee contacts. It also contains guidelines on what to do in the event of a disaster. Most of the IT crew (including the CIO) is also trained to bring up the system if needed. They also have a PR person for their east coast and one for their west coast to handle press, etc. in the event of a disaster.

The company's view is that 9/11 has not created much change in the business environment on the security side. The occurrence of virus attacks and the impacts they have had in bringing businesses to a halt are more relevant but diverse. For instance, that did not impact business but

did impact productivity was from a consultant. Since then, they have changed their practices and do not allow consultants to access their network. They have also installed greater level of security by using Microsoft's new active directory.

Overall, Company B is well prepared for business continuity in IT and reasonably prepared for business continuity as far as employees and facilities are concerned. Due to the nature of their business, their stores are geographically dispersed which offers them natural protection. Most of their assets are physical which are covered by insurance. Among their information systems, merchandising is most important, which they have prepared to recover in negligible time. However, it is the occurrence of viruses rather than the events of Sept 11 that has caused them to increase their security and pay attention to their business continuity plans.

Company C:

Company C owns a chain of warehouse type stores in California, Arizona, Nevada and Florida. It sells an assortment of bulk-sized foods and related supplies designed to appeal to businesses, restaurant businesses and household customers. The company was started in the late 1800s as a single grocery store in Los Angeles and grew into a very successful wholesale grocery store chain by the turn of the century. It survived its competition by pioneering the "cash and carry" concept in Los Angeles to cut costs and by locating its stores close to business. Today the company has 228 stores spread across in western United States and northern Mexico and has over $2 billion in annual revenues and provides employment to almost 5,500 employees.

Although only about 1.5% of the company's workforce is IT (information technology) and less than 1% of their total budget is devoted to IT, Company C has a strong IT infrastructure, a web site where customers can purchase products online, and have also recently installed digital receipts generation capability.

The company is also prepared for disaster recovery and business continuity. They have off-site data storage (storage on tape or disk to a different physical location) and maintain some cold sites (empty computer facility ready for computer equipment to be moved in). For their critical IT functions, they also do mirroring (maintain replica of their databases/file systems by applying changes at the secondary site in lock step with or synchronous to changes at the primary site) of the data. Company C has also had electronic vaulting (data sent directly from the subscriber to the hot site) to maintain business continuity in the event of a disaster for several years now. The company currently does not maintain any hot sites however.

Their business continuity budget over the next few years is expected to remain steady. Company C's perspective is that business continuity awareness among organizations had increased after the happenings of 9/11. However, this awareness has now gone down. Company C believes that this heightened awareness in business continuity after 9/11 was only a spike.

Most of the company's information technology functions are currently performed in-house. They have in the past tried outsourcing some of their IT functions overseas. However, that had not worked out favorably for them. They have however expanded their sales beyond the United States to Mexico as well as Canada.

Overall, the company is very aggressive with their brand. They use various methods to promote their brand awareness. One of the big accomplishments of Company C's IT division is the successful deployment of digital receipts. They can now retrieve any one receipt, which would take them 11 hours to retrieve in the manual system in 4 and ½ minutes. This alone has turned over the company's payment schedule from 34 days to 6 days. The company has also been able to cut down their labor costs significantly.