Business Continuity Planning

White Paper

Prepared by:

Upper Mohawk, Inc.

The Gartner Group recommended in a report published July 2001 that companies and government organizations should spend 3-8 percent of their budgets on a Business Continuity and Disaster Recovery Plans. Due to the September 11th attacks, the issue of Business Continuity Planning is being addressed globally. This paper, prepared by Upper Mohawk Inc. is designed to inform and to assist organizations in understanding the Business Continuity/Disaster Recovery Planning Process and to assist in preparing for an internal analysis for the creation of a Business Continuity Plan.

Table of Contents

Table of Figures

Executive Summary

Organizations in today's digital world rely more on technology and automation than ever before. Through technology, organizations have blazed the paperless frontier, bridged the digital divide, and made great strides in applying technology to everyday business processes. Organizations now span globally and have customers to support 24 X 7 X 365. With this level of automation, any breakdown in organizational information flow can cause a disruption in business continuity having a catastrophic effect on the organization's ability to support their customers and core mission.

With increasing reliance on information technology, the costs of interrupted access to data or the loss or compromise of customer data can impact an organization's functional ability and subsequently their reputation. This reputation, in private or government sectors, can be completely erased with just one devastating loss of business continuity. It is often impossible to place a dollar figure on the impact of business continuity losses, but an organization's ability to remain focused and operational throughout any disruption is what sets the organization above the rest.

Another factor in today's business world is ever increasing legal and government regulations. These regulations can have a major impact on an organization that is not diligent in protecting customer data or civilian privacy and maintaining business continuity

To appreciate the severity of such an outage, one must first understand that no organization is immune to business continuity interruptions. An outage or disruption to service can come at anytime and by any means including intrusion into systems by hackers, physical attacks, bioterrorism, terrorist attacks, accidents, equipment failures, or natural disasters. What allows one organization to survive such setbacks with their reputation intact, while others do not, is its ability to mitigate the obvious disruptions and have a well formulated plan to handle any other events. Even if the organization is only able to maintain the most basic of services or mission continuance, a well formulated plan during a disaster will give them the ability to continue where others have failed.

This White Paper is intended for Private and Public Organizations, Federal Government Agencies, State and Local Governments, or any organization that has an investment and reliance on Information Technology dependency to meet their core business and/or mission objectives.

At the leadership level, CIO's and IT Managers are concerned with protecting the organizational interests and investment in Information Technology and corporate data. Achieving service levels defined in service level agreements (SLA) with supported customers can only be obtained through a sound plan formulated by a company that has many years of successful business continuity planning.

Upper Mohawk Inc. (UMI) has extensive experience and knowledge in maintaining business and mission continuity. With years of successful support provided to the Department of Defense, State, and local Governments, UMI has formed a reputation in providing business continuity planning and services to customers with the most "unique" requirements and has experience in the handling of data from all levels of security classifications.

What this White Paper Provides

- Business Continuity Planning components as defined by International Standards Organization ISO 17799 compliancy
- Overview of the enterprise-wide Business Continuity Process
- Summary of various data availability and recoverability strategies and technologies, and the "value added" benefits derived by an organization through the implementation of those strategies
- Review of the various remote system's management and administration support services
- Upper Mohawk's experience and qualifications to implement cost saving and mission essential BCP practices into customer organizations

Business Continuity Planning as defined by the International Standards Organization

ISO 17799 was defined to assist organizations in counteracting interruptions to business activities and to critical business processes from the effects of major failures or disasters.

The sections of the ISO 17799 compliancy standard are as follows:

Section 1. System Access Control

The objectives of this section are to:

1. Control access to information
2. Prevent unauthorized access to information systems
3. Ensure the protection of networked services
4. Prevent unauthorized computer access
5. Detect unauthorized activities.
6. Ensure information security when using mobile computing and tele-networking facilities

Section 2. System Development & Maintenance

The objectives of this section are to:

1. Ensure security is built into operational systems
2. Prevent loss, modification or misuse of user data in application systems
3. Protect the confidentiality, authenticity and integrity of information
4. Ensure IT projects and support activities are conducted in a secure manner

5. Maintain the security of application system software and data.

Section 3. Physical & Environmental Security

The objectives of this section are to:

1. Prevent unauthorized access, damage and interference to business premises and information
2. Prevent loss, damage or compromise of assets and interruption to business activities
3. Prevent compromise or theft of information and information processing facilities.

Section 4. Compliance

The objectives of this section are to:

1. Avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements.
2. Ensure compliance of systems with organizational security policies and standards.
3. Maximize the effectiveness of and to minimize interference to/from (this wording seems awkward) the system audit process.

Section 5. Personal Security

The objectives of this section are to:

1. Reduce risks of human error, theft, fraud or misuse of facilities
2. Ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work.
3. Minimize the damage from security incidents and malfunctions and learn from such incidents.

Section 6. Security Organization

The objectives of this section are to:

1. Manage information security within the Company
2. Maintain the security of organizational information processing facilities and information assets accessed by third parties.
3. Maintain the security of information when the responsibility for information processing has been outsourced to another organization.

Why should I consider Business Continuity Planning

The world is a much different place than it was just three years ago, especially for business and the business of government. These days, most companies must operate in an “always open” mode—

providing continuity and total responsiveness around the clock and around the world. Where hours of operation used to be retail, business or banking, companies have become accustomed to dealing with global partners, work-at-home employees, and customers who are operating at any given time of day. For many companies, the urgent need for business continuity planning was brought into focus by the terrorist attacks in the United States on 9/11. While acts of terrorism are relatively rare, any company can be severely impacted by such an interruption. As mission-critical operations are moved to the Web, threats to information assets and systems are on the rise. Hackers, viruses, system overloads and Website failures are just some of the problems that could shut a company down. Information Week Research estimated that security breaches would cost businesses worldwide almost US$1.4 trillion in 2002…in fact that figure was surpassed!

What's really at risk? The impact of an operational interruption ranges from real revenue losses to intangible risks such as communications failures and customer dissatisfaction. Where two days of downtime used to be acceptable, companies have now significantly raised their requirements for business continuity. If a company cannot recover from a disaster in a timely way, the consequences can be devastating. According to recent studies, 40 percent of companies that suffer a business continuity disaster go out of business within two years. Even more devastating can be data loss or information exchange interruptions that affect the quality of peoples' lives or even their very own lives. .

However, business continuity management (BCM) has its own risks associated with it. "Disaster-recovery planning is a complex task, but organizations make it even more complicated by throwing everything but the kitchen sink into the plan," says Guy Baldauf, BCP subject matter expert for Upper Mohawk, Inc. "Such over complicating the process can lead to a plan containing hundreds of pages – creating analysis paralysis." History along with our experience demonstrates that a BCM plan needs to be a useable document. According to research by InformationWeek, almost 30 percent of companies surveyed are experiencing incidents that require the use of business continuity plans.

To ensure effectiveness, business continuity plans must be adopted throughout an organization in a proactive manner and make use of current tools and strategies. Storage back up, relocation or collocation planning, and distributing valuable assets across different geographic locations are just a few ways that companies can prepare themselves, their employees and customer relationships against a future crisis.

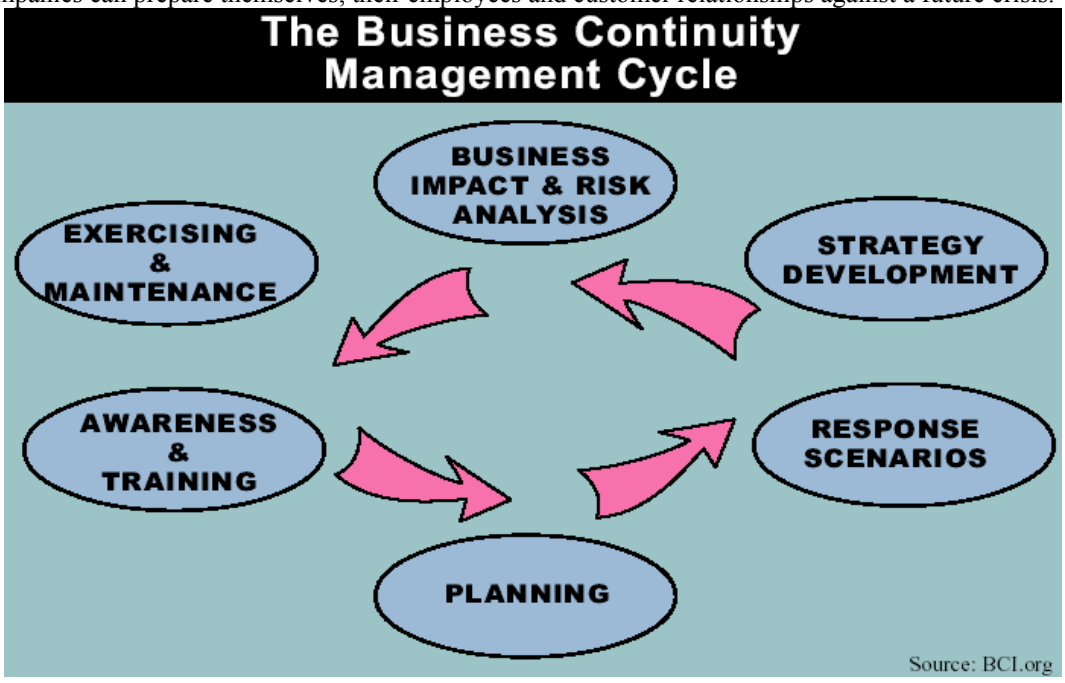
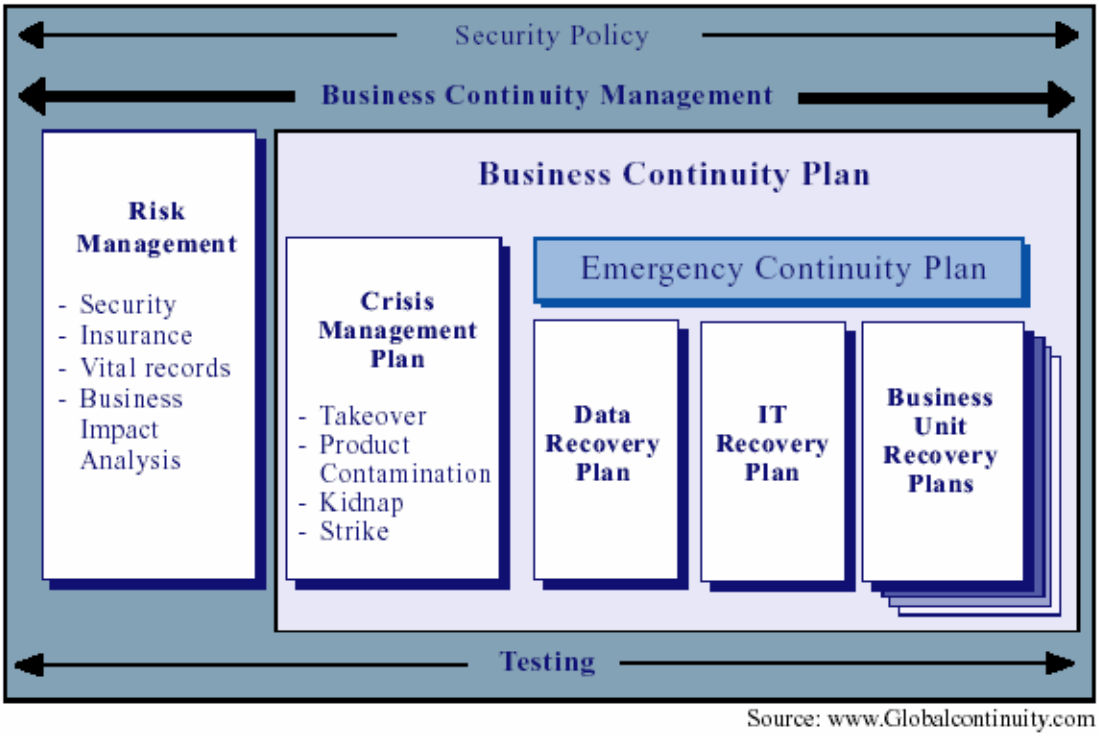


Figure 1 – BCM Cycle

As mentioned previously, the Gartner Group recommends that companies spend at least 3 to 8 percent of their IT budgets on a business continuity and disaster recovery plan. We at Upper Mohawk, Inc. believe that in most cases this is probably not enough due to the increase in the potential for terrorist attacks and the significant damage any business continuity loss can cause a company in today's competitive marketplace. To back this theory, and according to CIO Magazine's survey of IT professionals, more than half will increase their investment in IT contingency and disaster recover plans in 2004. Among the areas in which companies will increase spending are offsite redundancy (34 percent), offsite data/applications backup (31 percent), backup facility (25 percent), replacement equipment (24 percent), remote access (23 percent) and virus detection (23 percent).

Business Continuity Defined

Business continuity management, or BCM, is a set of plans that assists a company in restoring business operations under difficult or extreme circumstances. Unlike normal system outages, where business continues even though a system is down, business continuity comes into play when the business is at risk. Most companies are capable of solving small-scale operational problems that occur regularly in any business. However, BCM extends these problem-solving processes to severe situations on a large scale. Establishing and meeting BCM goals is not an easy or short-term project. We believe that less than half of corporations with a business continuity plan actually meet their recovery objectives. Business continuity is a high-maintenance proposition -- one that needs constant testing and updating throughout an organization. BCM plans vary, but most combine several common elements into a comprehensive strategy.



Source: www.Globalcontinuity.com

Figure 2 – BCM

Risk Management: BCM is actually an outgrowth of risk management, which originally was an actuary-based insurance approach to assessing risk. Risk management includes overall company security, making sure that valuable assets are covered by insurance, protecting vital records and analyzing the impact of a variety of events. Most companies conduct some level of ongoing risk management assessment.

Crisis Management: Crisis management is a strategic planning process for protecting the brand, image and/or reputation of a company. During crisis management, company executives need to manage communications to keep damage at a minimum. Crisis management usually focuses on specific areas of a company including public relations, human resources, facilities, and security.

Emergency Management: Emergency management produces a plan that protects a company's assets, resources and facilities. This is a detailed plan that spreads tactical decision-making throughout an organization. Emergency management creates communications liaisons between departments within a company and with emergency services outside the company. Emergency management includes:

- Data Recovery
- Technology Recovery
- Functional Recovery of Specific Business Units

Advances in technology have played a major role in providing the framework for maintaining continuity for e-businesses. According to InformationWeek Research, 98 percent of companies with a BCM plan include data recovery and 96 percent include technology recovery. These are the must-haves that allow a company to continue operating, regardless of the condition of a facility or the availability of the employees that work there. Data and technology recovery can be divided into several areas. The majority of companies have some sort of preparedness plan that includes some or all of these elements.

Back-up: Analysts estimate that 60 percent of a company's critical data is stored on individual laptops and desktops. Companies have long recognized the need for backup and have established elaborate systems that provide local backup and remote backup. Eighty-three percent of companies surveyed by InformationWeek have a backup process for departmental and application servers and 80 percent back up their data centers. However, only 64 percent provide back up for the data on PCs of individual employees and only 52 percent have plans for recovery of intellectual property.

New services will help solve this problem. Upper Mohawk, Inc. provides solutions for automated desktop backup and recovery to rebuild users' systems. These services can be used as primary storage or secondary storage.

Replication & Redundancy: Creating a mirrored copy of an entire data center is the most effective way to ensure business continuity. However, this is a costly proposition. With replication and redundancy, a company installs a mirror image data center, either at a separate location or co-located within the facility. Server and router switches are clustered at both the primary and secondary sites. This allows the primary site to continue to operate even if a server fails. Data needs to be protected at both sites with strong security.

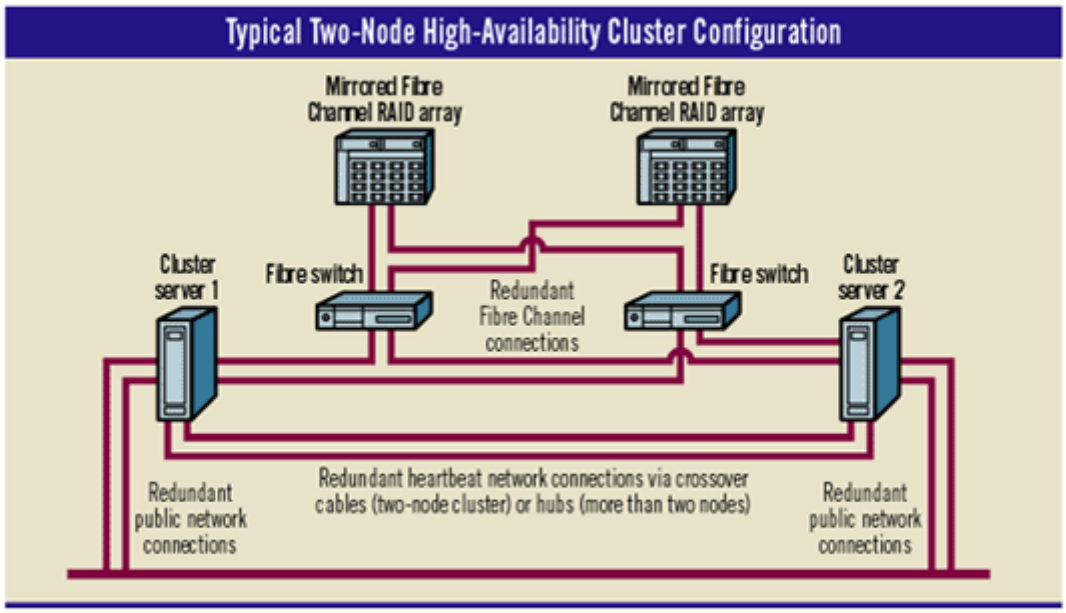


Figure 3 -- Clustering is one method of replicating data real time

Each site needs to be synchronized, to ensure that data is backed up on a regular basis and that both sites are operating with identical data. Operating system and application synchronization means that identical platforms must be maintained at each site. Data must be synchronized on a daily or weekly basis; or in the case of a transaction based business, instantaneously. Companies should make the decision to create a mirrored site at the beginning of a new installation.

Failover: Detecting an outage and switching to the secondary site is called failover. The detection of an outage can be automatic or can be identified by a human administrator. Failovers can be preset for situations ranging from a network interruption, a system overload, or hacking attempt. A comprehensive monitoring program can check for a failure at all levels and alert an administrator or automatically trigger the failover process.

Security

Since information is the most likely asset to be exposed to threats, companies have taken a close look at the way they protect their data and internal operations. New technologies allow companies to operate both as virtual, extended enterprises, and to provide a safe environment for transactions and communications.

VPNs, firewalls, authentication services and virus detection, are important services for business continuity. Companies are investing heavily in these technologies to improve the security of their data stores, communications, and transaction processing.

Increasingly, outsourcing services allow companies to hand-off these critical functions. Specifically, the outsourcing of redundant data centers and back-up locations are important developments.

Options

BCM and disaster recovery is not limited to restoring IT functions and recovering data. Rather, a comprehensive plan must include maintaining continuous operation of the data center, as well as the restoration of a company's overall business. This requires an integrated approach to BCM, which will ultimately allow the company to retain control of operations. Commercial recovery sites allow companies to use a data center and office space to continue their operations in the case of an emergency. These recovery sites fall into three categories:

- Hot Site: A hot site is a fully equipped, operationally-ready data center that is stocked with equipment specific to a company's needs. A hot site is ready for immediate use when disaster strikes. Company employees report to the hot site, instead of their regular office, and can begin working on equipment that fully replicates their office operations. Costs for a hot site are subscription based— a company pays hundreds of thousands of dollars a month to keep the site available for its needs.

- Cold Site: A cold site is a computer room and office space with electricity, phone jacks and hook ups, ready for equipment and employees to move in as needed. It is much cheaper than a hot site, running between $500 and $2000 a month, because the customer provides and installs all the equipment. It takes longer to become operational, but for a company that can't afford a hot site, or one that can afford some downtime, it is a reasonable way to prepare for disaster.

- Mobile or Porta-Site: For smaller computer installations, companies can contract with a mobile site provider, which provides a standalone computer and office environment, usually on a mobile trailer. Porta-sites are transported and constructed quickly at the site of a company. These sites usually cost the same as a cold site, but bring the work environment to the end user.

Upper Mohawk, Inc. can provide the expertise and services for companies and government organizations to develop an integrated BCM plan consisting of any of the above named technologies.

Challenges

Although the need for disaster recovery and BCM plans are well recognized, they still face challenges. Possibly the largest is the fact that most companies neglect preparation in lieu of dealing with immediate problems. Acknowledging that a disaster can happen to anyone can be a huge obstacle when compared to the "business fires" of the moment.

Secondly, BCM can be expensive especially when top management does not fully acknowledge the potential for business continuity disasters and is wrapped up in the reactive day to day company operations. Developing a mirrored data center, installing data back up systems for all employees and

ensuring network availability at all times is not cheap, but the alternative can be devastating. Hot site costs are even more exorbitant; in fact, a comprehensive back-up system can be viewed by companies as an expense for equipment and services they may never need to use.

The third major challenge for BCM adoption is the scope of the project. The World Trade Center attack lifted the bar for BCM services, moving the requirements beyond data center recovery toward a more integrated approach. In order for a BCM plan to be effective, it must incorporate inputs across an organization and take into consideration the functional needs of all mission critical departments. Once a plan is established, it must be constantly tested and managed.

Analysis, Analysis, Analysis, How Do We Get There

A key ingredient to implementing a successful BCP development project is to obtain corporate and management "buy-in" to support the BCP effort. Once this is accomplished project awareness within the rest of the staff must be established in order to move forward with the project objectives and requirements definition phase.

Once developed and initiated the BCP plan should be considered a "Living Document". This document can and should become the cornerstone of the organization. A company's BCP plan should always be updated and become part of an organizations configuration management process. The introduction of technology, changed vendors or suppliers, or any other changes in methodology should be reflected immediately in your BCP.

The methodology to developing a sound, functional BCP is a five-phased approach. Highlights of each phase include:

1. **Initiation.** This is the process of laying the foundation to the BCP process. The objective in this phase is to develop the overall strategy for the BCP program. This includes development of the BCP Program organizational team structure, definition of roles and responsibilities, establishment of the BCP budget, identification of stakeholders, and securing management "buy-in".

2. **Risk Analysis.** In this phase you will interview your key business and information technology experts. During this interview phase you will: define all key business processes; develop scenarios to define disasters that can impact your key processes; inventory all key business processes; and define how each scenario impacts that process. Also, the organization will need to define all interdependencies of key processes and how a loss of each key element affects the rest of the organization. An analysis of current recovery capabilities, security procedures, and a review of your organizations configuration management procedures are provided in this phase.
3. **Detailed Analysis.** During this phase a Business Impact Analysis (BIA) may also be completed depending on the scope and objectives of the project as defined by the customer during the initial phase of the BCP development project. A completed BIA may help in deciding the scope of the BCP coverage and obtaining a champion to secure funding for the project. A thorough understanding of the customer services and Service Level Agreement(s) (SLA) along with the knowledge of customer staffing and regulatory constraints is required for this phase. A Threat Analysis can be completed in parallel to the BIA to determine potential threats to the customer site, and to begin work to mitigate those threats according to the probability of occurrence and extent of the damages associated with the known or discovered threats. A Business Process Gap Analysis and Technology Gap Analysis are developed to close the "Gaps" identified in the Risk

Analysis Phase. Also a "Current Business Snapshot" is taken to ascertain the current standing and capabilities of the organization. During the BIA process an assessment of the security posture, policy, and guidance should be evaluated as part of the threat assessment. Lax security or lack of an on going IA program/Vulnerability Management effort is a definite threat and can lead to serious Business Impact (down time, increased labor, analysis, and recovery).

4. **Remediation / Development.** This is the phase that develops the actual BCP plan. All findings from the Gap Analysis are implemented to close the Gaps. In parallel to this process a DRP plan will also be developed to address information technology systems and their recovery. All associated documents are updated, including Service Level Agreements, business partner agreements, and vendor contracts; updates are made to reflect the strategy provided in the BCP plan for the organization. Establishment of Off-Site Storage, Alternate or Hot Site facilities and other contracts are finalized with appropriate support organizations. The testing of the plan and all remediation of action items are wrapped up.

5. **Document Maintenance.** Ensuring that these documents and plans are always updated is a key element addressed in this phase. Scheduled testing, audits, and reviews are performed to ensure the accuracy of the plans. The organization's configuration management procedures should be updated to ensure this document is kept current and ready to be executed. Business processes should also be updated as well as any personnel changes to key personnel.

Upon completion of the aforementioned steps, BCP documentation will be developed to capture the scope, objectives, constraints, limitations, and recovery requirements necessary to successfully recover the critical environments or functions identified.

These strategies and processes can range from developing a plan to recover a single system and/or application to one that is developed for an entire production environment. They may also target partial or full Business function recovery as well. Services and strategies must be tailored to the requirements, recovery objectives, and available customer funding. They may include physical or electronic Off-Site Data/Image Storage, Cold or Warm Site recovery processes, or implementing variations of strategies to ensure Recovery Time Objectives[1] (RTO) and Recovery Point Objectives[2] (RPO) are achieved. The customer should also decide on mission essential data where the implementation of Hot Site strategies are encouraged to ensure immediate "fail over" or "mirroring" capability to mitigate critical IT outages. Additionally, alternate site strategies can be developed and implemented to return personnel to work in a suitable office environment with the necessary support to execute daily business functions.

Additional Continuity Options

The next section is devoted to other technologies and methodologies not previously discussed that can be implemented to complement a successful BCP / DRP plan.

Off-Site Data Storage

Off-site Data Storage is a critical requirement to support an effective BCP. This is normally accomplished by providing a physical storage and rotation plan of system/application back-up media such as tape. A 'Recovery Time Objective' (RTO) of 72 hours is generally achieved with this strategy and a designated alternate site to execute recovery. Off-site Data Storage is a much cheaper undertaking compared to other more elaborate back-up methodologies and certainly far less of a cost and impact vs. possessing **a complete inability** to recover. The RPO may mandate a requirement to restore a system/application to current time with minimal or no data loss. In that case, it would require additional time to bring the architecture forward to the current time of the outage from the time of the last back-up of restored data. In some instances, depending on the availability of incremental data following a restore from the full back-up, catch up processing (data/transaction reentry) may be required to minimize data loss and to bring the system to current time. It is strongly recommended that the Off-site Storage area include (in addition to back-up data) copies of environment software, license, certificate information, vendor documentation, a copy of the BCP, additional back-up media (tape, CD, DVD, USB drives, etc.). The storage area must incorporate environmental controls to ensure stability and reliability of the stored media and must meet security requirements. Variations of this strategy may include storage of peripheral drives (USB) that store complete server/host images refreshed (over written) and rotated much in the same manner as tape media, greatly reducing the restoration window of the recovery operation and concurrently reducing the RTO. CD and DVD media can be implemented for smaller hosts and images in place of peripheral drives. This is generally a low cost proactive strategy that serves as a foundation to the BCP.

Considerations to this strategy include, but are not limited to:

1. **Classification of the data or media.** This may increase costs as the classification level increases with the corresponding increase in impact severity to National Security. This requires additional Security implementations at the storage facility and personnel with proper security clearances to handle, ship, and execute the restoration.

2. **Recovery team staffing requirements**. The methodology of retrieving data from Off-Site storage and executing a recovery at an alternate site requires the maximum amount of staffing in most cases. Each area of expertise and each discipline must be present and knowledgeable of the target environment to execute a recovery from tape/media. This is in part due to the requirement to "build" and configure recovery hosts, servers, network connectivity, etc. and requires manual intervention of a knowledgeable recovery team. Always consider that the impacted organization may not be able to provide recovery team staffing due to injury or loss of personnel, inability to travel/communicate, etc. The recovery team staffing requirement may be reduced through the utilization of image storage methodologies which in turn reduce the amount of manual configuration of the target environment.

3. **Travel and distance to the Off-Site Storage Area and Alternate Site.** This is an area each organization must consider prior to implementing Off-Site storage. If possible, match the Off-Site storage area with the designated alternate site or utilize a facility that may be on the transit route to the alternate site facility and has staffing available to move the data to the alternate site upon proper notification. In addition to this, the designated recovery team members should arrange for access with the Off-Site storage facility to gain access to the data if required on a 24X7X365 basis. Off-Site data storage may be by electronic means and stored in a SAN or similar environment whereby the alternate site would have access to that back-up data and with proper notification and authorization would retrieve the data from the storage environment via electronic transmission to the designated recovery hosts in the event of an emergency.

Alternate Site Support (BCP)

There exist many degrees and variations of this type of BCP support. A designated Alternate Site should have the capability to support initial and on-going testing of the BCP through the Life Cycle Management of the project. Several key areas of the Life Cycle Management of the BCP project must include data growth metrics to support current and future capacity planning, cost of data management, on going assessment of the cost of down time/data unavailability, and projected IT growth within the supported organization.

In addition to the required testing, it may be possible for the Alternate Site to support hosting of the required recovery assets and if documented, configured, and tested, this may reduce the RTO to 24 – 48 hours depending on the number of systems/applications targeted for recovery, the amount of data to be restored and/or retrieved electronically, and available bandwidth to move the data to and across the recovery environment. With additional configuration executed, tested, and pre-staged at the Alternate Site RTO may be reduced to a range of 8 - 24 hours, again depending on the scope of the recovery environment and amount of data targeted for restoration.

Through this method of BCP support commonly referred to as "Warm" Site support, pre-configuration and testing of the Alternate Site may reduce recovery team staffing as well as reduce the probability of human error that can be experienced during an actual emergency. Keep in mind that during an actual emergency, employees may not be able to support key roles in the recovery operation and this "Warm" site strategy/methodology reduces the impact to those instances.

The initial Alternate Site support may only target the most critical Customer systems/applications or it may address the entire data center floor. Alternate Site support is also critical to support internal Business function continuity and will require assessment of the Primary Site requirements, staffing, etc. to ensure successful Business Continuity Planning. Business Continuity recovery should be tested. This test must address the operational recovery along with strategies to notify and move key personnel to the Alternate Site, and account for the administrative and financial support of those personnel designated to support the recovery. Every effort must be made to recognize even the smallest details like office automation requirements, consumables, and a coordination strategy to ensure organizational cohesiveness with the Alternate Site. A second Alternate Site strategy to support recovery of operational assets involves the availability of Storage on Demand (SOD) and Processing on Demand (POD) whereby vendors will place the necessary resources at an alternate/reciprocal site and there will be no charges levied until those additional resources are utilized. A thorough capacity planning effort must be completed to ensure the standby resources are sufficient as well as some testing to ensure configuration of the primary site can be accomplished in the target environment. A cost analysis of this should be completed and requires full participation of the vendors providing assets. This same strategy can be utilized to support "fail over" processing capability and with the proper front end planning and testing can provide excellent emergency response recovery and reduced RTO windows.

The next major phase in Alternate Site support is data replication/mirroring. Without the backend data, all front-end processing is virtually useless. A cloned processing environment can be accessed within minutes and/or as much as hours following an impact to the primary processing facility. This depends on the extent of parallel processing implementation and time latency of the data replication. These strategies can be tailored to provide a well balanced solution that meets all of the customer's requirements no matter the complexity of the environment.

As stated there are a number of variations to the Alternate Site strategy, one is a "Cold" site agreement where a raised floor is provided that will host recovery resources in the event of a primary site outage. This strategy can include the provisioning of hardware by the host site, or the customer can bring the equipment when reporting on-site. This strategy fits the needs of those customers who do not have a critically short time to recover or return to operational status. One must keep in mind that this strategy can be very difficult and costly to implement unless guided by a sound BCP plan. With the right guidance a remote "Cold Site" recovery can be accomplished within a very short time frame. Once again, the timeframe required for the recovery is the main delimiter in the cost and complexity of the plan.

To make any plan a complete success, you must establish sound Life Cycle Management and Configuration Management processes that include your BCP/DRP planning and methodology. This will ensure that every phase of the plan will always reflect your true production environment. This in turn will justify the BCP dollar expenditure to the organization and provide tangible, measurable results.

As indicated in the previous discussion, recoverability and information assurance can mean the difference when an organization's reputation or market name is at stake. The loss of that reputation can often lead to the financial disaster of an organization. This can even extend into regulatory impacts, impacts imposed by Federal or Presidential Executive Orders, and the loss of an organizations legal means to fulfill its Mission Statement or services offered. With proper, thorough planning and testing the necessary assurances can be established and implemented to avert, mitigate, and minimize these impacts.

The data in the table below illustrates data provided by the Fibre Channel Industry Association (Oct 2003) and demonstrates the high cost of IT outages and offers some insight on the estimated dollar loss for hourly down time relevant to some of today's Industries.

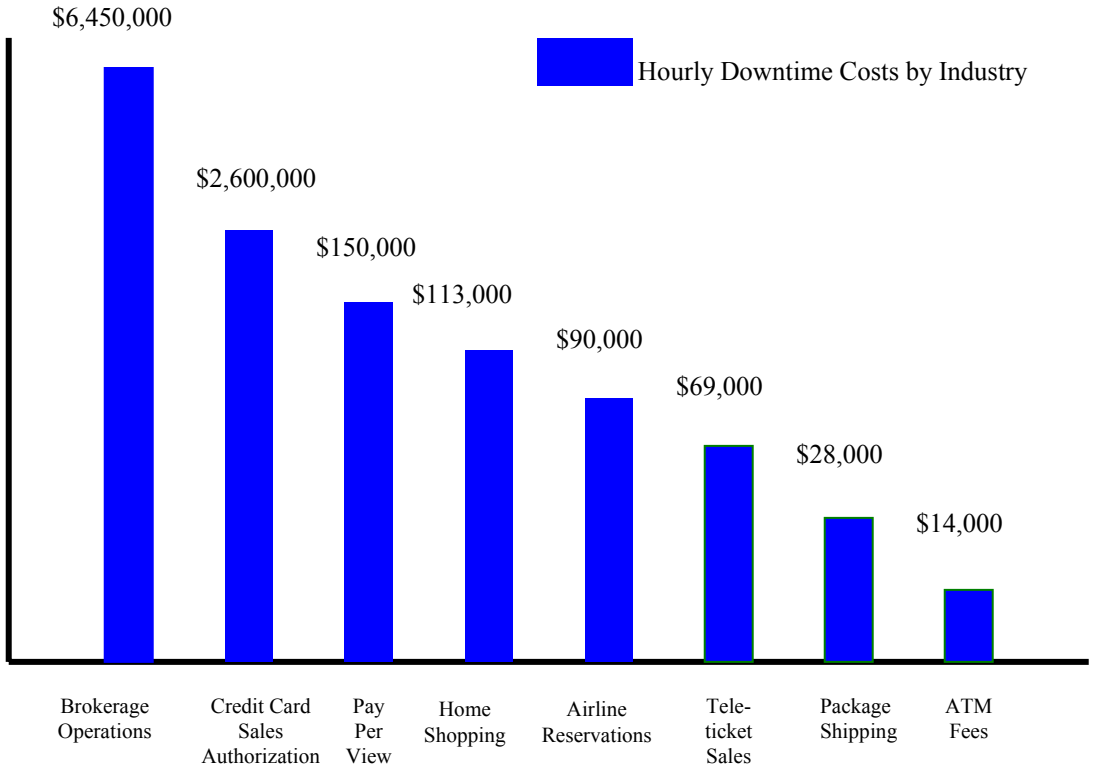


Figure 4 – Hourly Downtime Costs

Throughout the BCP process it is important to keep in mind that data recovery does not conform to a specific model. Recoverability is driven by the need to implement technologies based upon the specialized requirements of the Customer. Rather than implementing a specific model, a cost effective common sense approach is taken to apply a combination of optimal technologies to achieve the Customer's objectives within budgetary constraints. The listing below provides an overview of some of the availability, recoverability, management, and resource multiplying technologies available in today's technology marketplace. These must be assessed and mapped to the Customer business requirements based on cost, maintenance requirements, RTO and RPO objectives, organizational growth, etc.

- Block Level Back-up
- File system data snapshots
- Data replication
- Open File back-up
- Point in time, off host, mirroring
- Removable media back-up (Tape, USB Drives, CD, and DVD)
- LAN Free back-up
- Remote SAN
- Full system imaging
- Back-up to disk
- Remote fail over systems
- Centralized back-up administration
- Warm Site hosting
- Reciprocal site agreements
- Workstation back-up
- Communications, network, server redundancy
- VM software
- Bare metal system restoration

The list above is just a sampling of the numerous technologies that can be applied and integrated into any plan. Each technology has particular advantage that brings additional value if used correctly and matched properly to the environment.

Considering all the complexities in BCP planning and implementation, it is important to select a company that has successfully demonstrated a strong past performance with a winning track record. UMI possesses the skill and experience to successfully develop and implement any BCP/DRP plan or services. UMI is a company that can take you through all phases of the BCP development and provide the on-going support to the Customer through the BCP Project Life Cycle. Through the implementation and use of Service Level Agreement(s) (SLA) with the Customer, the SLA act as a metric to help measure contract performance for both parties and can be evaluated to ensure the levels of service(s) identified in the SLA are provided and executed as defined. UMI has successfully provided services to some of the top Department of Defense and Federal Organizations. By working with the some of the most complex and critical environments, UMI has gained experience and knowledge that can turn any plan into a success. Some of our customers include:

- Defense Finance and Accounting Service (DFAS)
- Naval Facilities (NAVFAC) Information Technology Center (NITC)
- Fleet Industrial Supply Center (FISC)
- Naval Supply (NAVSUP) Command, Mechanicsburg, PA
- Naval Surface Warfare Center (NSWC), Crane, IN
- DISA Financial Management Liaison Office (FMLO)
- Defense Information Systems Agency (DISA)
- Naval Space Warfare (SPAWAR) Command
- Commander Naval Region Southeast (CNRSE)

Other Services and Support

Many organizations and Federal Government Agencies are operating in a challenging environment to minimize cost, reduce overhead, and accomplish more with no increase in personnel. Many of these organizations are turning to outsourcing Information Technology services or projects. This includes network or enterprise security and management.

UMI has the experience and expertise to support a variety of Customer Information Technology needs including:

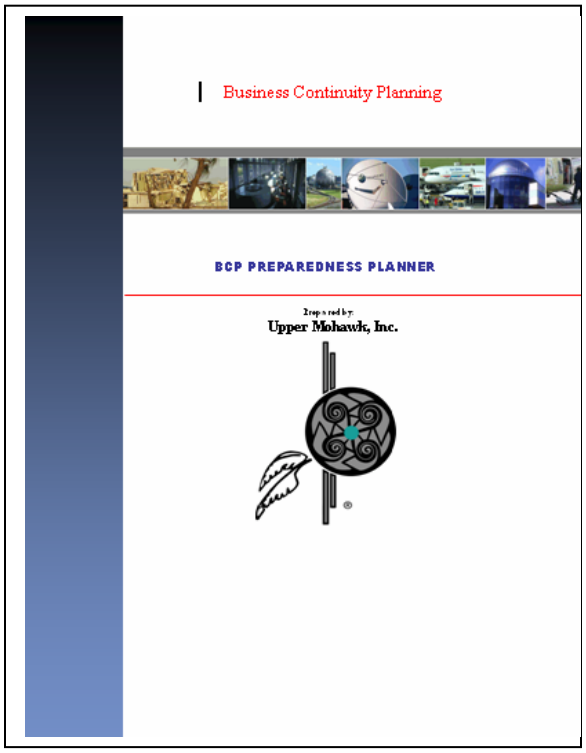
- Operational Support: level 1 and 2 Application recovery support, LAN/WAN Administration, Software Engineering Support, Telecommunications Support, Configuration Management Support, Portal Support, Software Life Cycle Support, Email Office Automation support and development, Active Directory design and support, Legacy System conversions and support, On-Site workstation support, and Help Desk Support
- Citrix Engineering Support: Application development, server administration, technology refresh

- Program Planning: Milestone tracking, Migration Support, Cost Analysis and Risk Management
- Web Development (Internet, Intranet, Extranet) and Administration: Interactive web design, On-line training, E-commerce, Advanced search tools, Information Management, Web and enclave security
- Certified Microsoft Engineers, Citrix Enterprise Managers, Cisco Engineers, and Certified Microsoft Developers
- PKI Security, Biometrics, Secure System Development

Summary

For most organizations or companies, investing in disaster recovery and business continuity will be a difficult challenge. Not only do funds have to be allocated during tight economic times, but a comprehensive plan must be developed. No longer are organizations protecting a specific department or function, such as finance or manufacturing. Rather, the entire organization must be involved in the planning of business continuity to ensure that all interdependencies are considered and addressed. The attack on the World Trade Center has put business continuity management in the spotlight. It provides a reminder that disaster can strike any company at any time. With the assistance of new technologies, specialized service providers, and a growing awareness of the need for a BCM plan, companies can prepare themselves and protect their information and employees against future threats.

As with other IT support services today, Information Security and Information Systems Security is of the utmost concern. Any organization or agency operating in an IT environment today is faced with numerous Federal, State, organizational, and regulatory compliance issues that demand full compliance and dedication to that effort. UMI has worked closely in conjunction with DoD CERT, DISA Field Security Office (FSO), Vendors, and the supported Customers to ensure that the highest levels of Information Assurance are provided. This is achieved through implementation of security guidance publications such as the DISA Security Technical Implementation Guides (STIG), and guidelines provided by the National Security Agency (NSA).



For more information please contact:
Ken Barnes
Upper Mohawk, Inc.
Phone: (888) 436-1814
kbarnes@uppermohawkinc.com