

The top section of the cover features the Systems Alliance logo in white, with the tagline 'Think Big. Work Smart.' in yellow below it. The background is a dark teal gradient with faint, glowing digital patterns and data points. A large, bright lightning bolt strikes a dark, stormy sky on the left side of the image. On the right, a blurred image shows two business professionals in suits walking through a modern, brightly lit hallway with a curved ceiling.

SYSTEMSALLIANCE

Think Big. Work Smart.

Disaster Recovery Planning - *Risks Uncovered*

January, 2006

Author: Ed Coram
Director, Professional Services
Systems Alliance, Inc.
www.systemsalliance.com

Table of Contents

Introduction 3
Risks Uncovered..... 3
Implications and Lessons Learned 4
Reducing the Risks..... 5
How ready are you – A Self Assessment 7
Reap the Benefit..... 7

Introduction

In a recent survey of IT professionals, 40% of the respondents expressed concern about their ability to recover from a disaster and almost a third claimed not to have a DR solution in place. The reasons given included lack of budget and other business priorities. Source: Continuity Central, June 2005

Where does disaster recovery rank amongst your top priorities? How much disruption can your business afford? For those readers who may be thinking disaster recovery is only a significant concern for banks and other financial services institutions, note the following statistic: **More than 50% of all businesses experiencing a major disruption do in fact fail.** Source: Gartner Group

In this white paper we identify risks uncovered and lessons learned in the wake of the weather and terrorist related events that occurred in 2005. In addition to describing the steps you can take to mitigate those risks, we also provide a quick self-assessment tool you can use to gauge your current level of disaster readiness.

Risks Uncovered

In the wake of 9/11, many businesses made the commitment to revisit and shore-up their disaster recovery plans. Two years later, after blackouts hit major eastern U.S. cities, 60% of U.S. IT departments said they had no formal plans or procedures in place to deal with the blackout.

With the recent increase in natural and man-made disasters you might expect to see many more businesses than you do with effective disaster

recovery and business continuity plans. In 2005 FEMA recorded 140 weather related disaster and emergency declarations in the U.S. alone. The U.S. State Department reported a three-fold increase in terrorist activity in 2004, as compared to 2003, the last full year for which data is available. Additionally, there has been no decrease in disruptions caused by hardware failures, critical application failures, inadequate IT and information security safeguards and, of course, human error.

While more businesses have disaster recovery and/or business continuity plans in place today than had them prior to 9/11, a surprisingly large number still do not. For those that do have DR plans in place, recent experiences have uncovered a number of key issues that are not being addressed:

- Those events most likely to have a significant negative impact on business operations (e.g. loss of a facility or the inability to gain access).
- The potential for long rather than short term dislocations (e.g. the need for an alternate site for more than a few days/weeks).
- The impact of business and technology changes on the defined disaster recovery plan and processes (e.g. recently deployed applications and/or infrastructure not reflected in the plan).
- The possibility that the firm's disaster recovery vendors will have their supply chains disrupted (e.g. the delivery of fuel for the vendor generator is delayed).
- Key personnel misunderstanding their role in the recovery process (e.g. a critical business resource being unavailable to validate an application restore operation).

Implications and Lessons Learned

1) Does the plan assume worst case scenarios?

As strange as it may seem, some disaster recovery plans don't address major service disruptions, planning to address minor events instead. Plans routinely anticipate a short term loss of power but less regularly account for the loss of access to key facilities.

One Systems Alliance client, a major university in the gulf coast region, hadn't planned for anything of the scope of hurricane Katrina. The good news was their data center wasn't impacted by flood waters. There was, however, significant humidity related damage. In addition, the CIO reported the university's communication plan was not as robust as it needed to be. He also noted that while systems had been backed up and arrangements made for the evacuation of back-up tapes, the tapes were stored in a downtown building that was locked before the pickup could occur.

Lesson Learned: To be fully effective, the disaster recovery plan should assume your building will be damaged, you can't take anything with you and you can't gain access to the building.

2) Does the plan address long term disruptions?

While most disaster recovery plans recognize and address the potential need for quick access to a hot site and/or other short term accommodations, many plans don't address the steps required to move to longer term accommodations. A typical agreement may allow for up to six weeks in a hot site and the plan for ordering, installing and testing equipment for the move to a cold site

or a more permanent location is best developed before a disaster occurs rather than in the midst of one.

As quite few firms in the gulf region will discover, if they haven't already, their hot site agreements are likely to expire before their primary facilities will again be available for occupation. For those firms that haven't anticipated the steps required to transition to long term accommodations, the trauma of hurricane Katrina will continue.

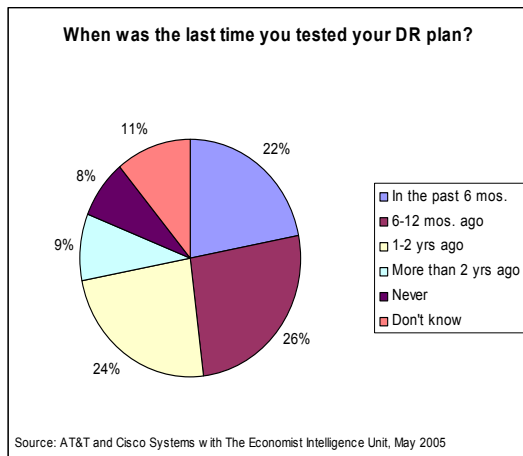
Lesson Learned: An effective disaster recovery planning process will consider the potential need for long term as well as short term accommodations. That said, the cost of the arrangements made must be balanced against the potential impact on revenue.

3) Does the plan reflect changes in the business and IT environments?

As we review the experiences of businesses in the regions impacted by hurricanes Katrina and Rita, the good news is that many of them did have disaster recovery and/or more comprehensive business continuity plans in place. The bad news is that many of those plans were not fully operational; they had either not been tested in the recent past or had never been tested.

As the below shows, most organizations that develop DR plans test them infrequently, if at all. In contrast, most organizations do not remain static. Business processes and application systems change, as do people, underlying hardware and software. While DR plans can be modified to reflect changes in the environment and people trained as roles and responsibilities change,

without testing there is no way to know it will work when required.



The importance of testing DR plans is depicted in the results of a March 2005 survey by the Chartered Management Institute. 100% of survey respondents who had implemented a disaster recovery plan and rehearsed it at least every six months experienced an effective reduction in the impact of disruptions.

Lesson Learned: The only way to assure the DR plan will work when a disruption occurs is to test before implementation, test regularly and test thoroughly.

4) Does the plan reach beyond the boundaries of the firm?

When a business disruption occurs, particularly when the cause is a major disaster, it is not unusual for restoration to hinge on the capabilities of a business partner or external service provider. Just as employees, applications systems and hardware components are considered when examining disaster recovery plans for single points of failure, service providers should also be included and contingency plans developed.

In the wake of hurricane Katrina, some businesses were unable to resume operations because vendors relied on for recovery services were,

themselves, unable to deliver. Today, companies are increasingly evaluating service provider business continuity and disaster recovery plans as part of the selection process for critical services.

Lesson Learned: For services deemed critical to the recovery process, relationships should be developed with multiple service providers.

5) Does everyone understand their role in the event of a disaster?

In response to a Disaster Recovery Journal survey question, 2,933 of 3,996 respondents (73.42%) indicated executives in their companies were not trained on what to do in time of a crisis. The CEO of a major construction services company cited the lack of a playbook that all responders could follow as a key reason for the government's failure in responding to hurricane Katrina. In order to respond effectively during business disruptions of any sort, companies also need clearly defined processes, procedures, roles and responsibilities. Every person involved in recovering from a disaster must know exactly where they need to be, what they are expected to do and who they should communicate with.

Lesson Learned: Define and communicate recovery related roles and responsibilities to all responsible staff and involve them in periodic tests of the disaster recovery plan.

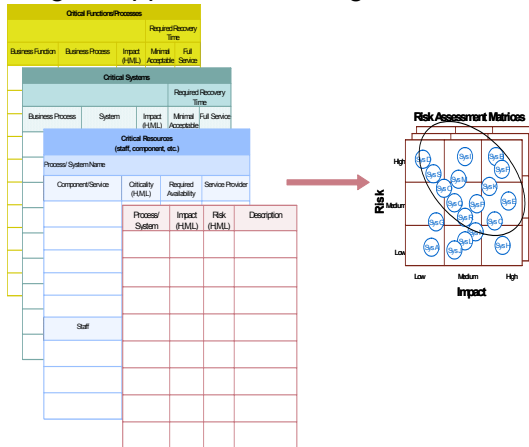
Reducing the Risks

We believe organizations can enhance their ability to recover from business disruptions, whether caused by a major disaster or a localized

event, by using a disciplined approach to disaster readiness.

I. Risk/Impact Assessment:

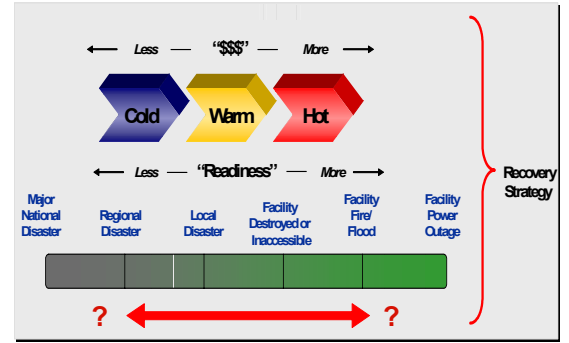
Evaluating risks and their potential impact on the business is key. However, understanding what might happen is not enough.



Businesses must also have a complete view of their portfolio of business processes and supporting technologies and understand the relative importance of each to the survival of the business.

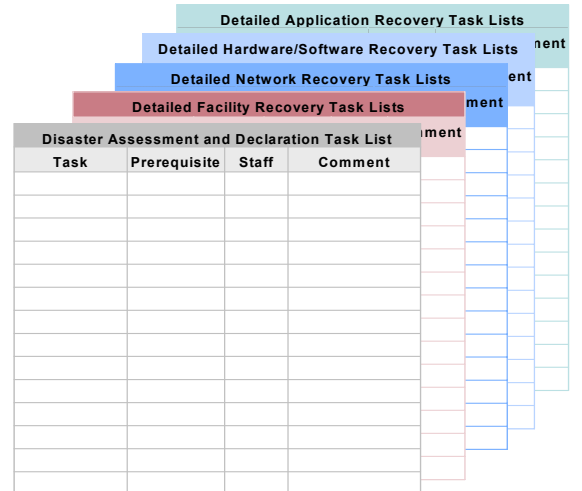
When Systems Alliance works with clients, we leverage structured tools to help them identify and assess risk and document the importance of processes and supporting systems in terms of impact on revenue. The assessment process aids the development of short and long term recovery strategies and plans. The view developed also helps the business make informed decisions about how much to invest in disaster recovery and where to focus its investments.

II. DR Strategy Development: In consideration of the risks identified and the relative importance of the business processes and enabling



systems, the organization must then develop a disaster recovery strategy that balances the threat level, alternative levels of readiness and the cost to provide each level of readiness.

III. Deployment Planning: What good is a strategy without an implementation plan? Once the strategy is developed, the organization must define the activities required to activate it. These include required changes to process, infrastructure and staff. The implementation plan also



addresses changes to service provider agreements and/or the establishment of new relationships.

Additionally, the planning process includes the definition of tasks, roles and responsibilities required to recover after a disaster as well

as those required to validate the plan.

IV. Plan Testing and Deployment:

Testing is a critical step in the deployment and maintenance of a disaster recovery plan. To be considered effective, the plan must be thoroughly tested and evaluated on a regular basis (at least annually). Procedures to test the plan should be documented. Thorough, periodic testing provides the organization with the assurance that all necessary steps are included in the plan. Testing also assists in determining the feasibility and compatibility of backup facilities and procedures, identifying required modifications, and providing training to responsible managers and staff.

How ready are you – A Self Assessment

How can you determine your level of preparedness for a major disaster? Here is a quick self assessment that should help answer the question.

#	Quick Assessment	Yes	No
1.	Does disaster readiness have support of top management in your organization?		
2.	Have you conducted a business impact analysis to quantify and rank the business and financial risk of disruptions to all vital functions?		
3.	Do you have a written disaster recovery plan that includes back-up and archive procedures?		
4.	Have you tested your plan using a worse case scenario (e.g. loss of facility)?		
5.	Did testing prove you could meet all recovery time requirements?		
6.	Have you taken action to mitigate known risks and single points of failure (e.g. power loss, physical access, etc.)?		
7.	Are you prepared to address liabilities and fiduciary responsibilities in case of disaster?		
8.	Is your disaster recovery plan updated regularly to keep it current with business and staffing changes?		
9.	Do you have an adequate budget to support your disaster recovery program?		
10.	Do you understand your disaster recovery costs, options, and disaster declaration procedures?		

If you answered no to one or more questions, you have some work to do.

Reap the Benefit

Despite the number of recent natural and man-made disasters, and the resultant albeit inconsistent increase in the attention to disaster readiness, organizations continue to experience shortcomings in their disaster recovery plans. We have described a number of those shortcomings, the related risks and the actions organizations can take to reduce those risks.

Following the steps outlined to develop and implement a comprehensive disaster recovery plan can produce a wealth of benefit, including:

- Limiting the economic impact of business disruptions
- Decreasing potential exposures
- Reducing the likelihood of disruption
- Enhancing organizational stability
- Providing an orderly recovery
- Reducing insurance premiums
- Decreasing the reliance on a small number of critical staff
- Protecting the assets of the organization
- Ensuring the safety of personnel and customers
- Enhancing the quality of decision-making during a disastrous event
- Minimizing legal liability.

For more information or to schedule a rapid disaster readiness assessment contact ecoram@SystemsAlliance.com

Ed Coram is the director of the Systems Alliance IT Performance Improvement practice. He has 25+ years experience in large scale IT environments and has successfully managed IT Improvement and cost savings programs for Fortune 1000 companies across a wide range of industries.

Systems Alliance, founded in 1993, is a Maryland-based company providing software development and consulting services to solve complex technology and business problems for corporate and public sector clients. Their clients include McCormick & Company, Johns Hopkins Institutions, Random House, Inc., GATX, Provident Bank, Loyola College in Maryland, and the Maryland State Department of Transportation.