



UNIVERSITY of HAWAII®  
MĀNOA

# Disaster Recovery & Business Continuity



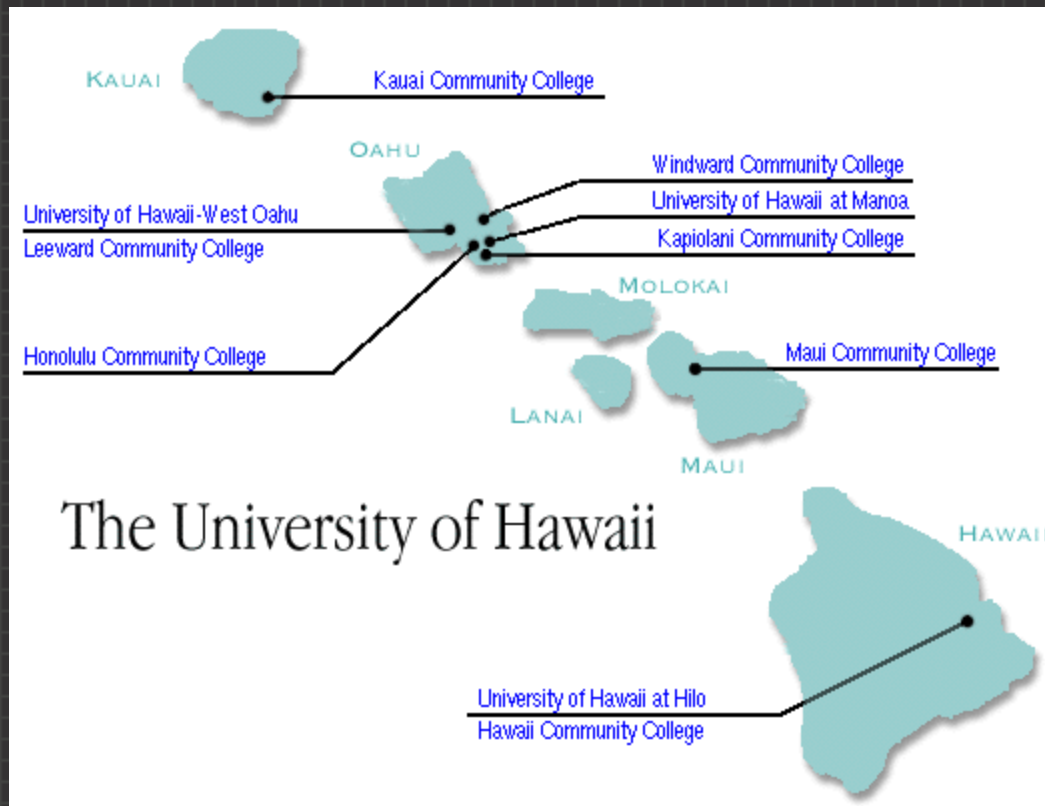
James Adamson  
Library Systems Office

# Library Management Information Data Services



- Financial
- Procurement
- Cataloging
- Inventory/searching
- Circulation

# Central Library Management Information System



# External Sites



# Disaster Recovery Plan

## **Disaster Recovery Plan**

Recovery and Continuation  
of Automated Library Functions  
at University of Hawaii at Manoa Libraries



**Systems Office**  
University of Hawaii at Manoa Libraries

- 1989
- Not taken seriously
- Complex
- Threat
- Budget
- Keep it up to date

# Disaster Recovery Plan

Recovery and Continuation of Automated Library Functions at the University of Hawaii at Manoa Libraries

## Table of Contents

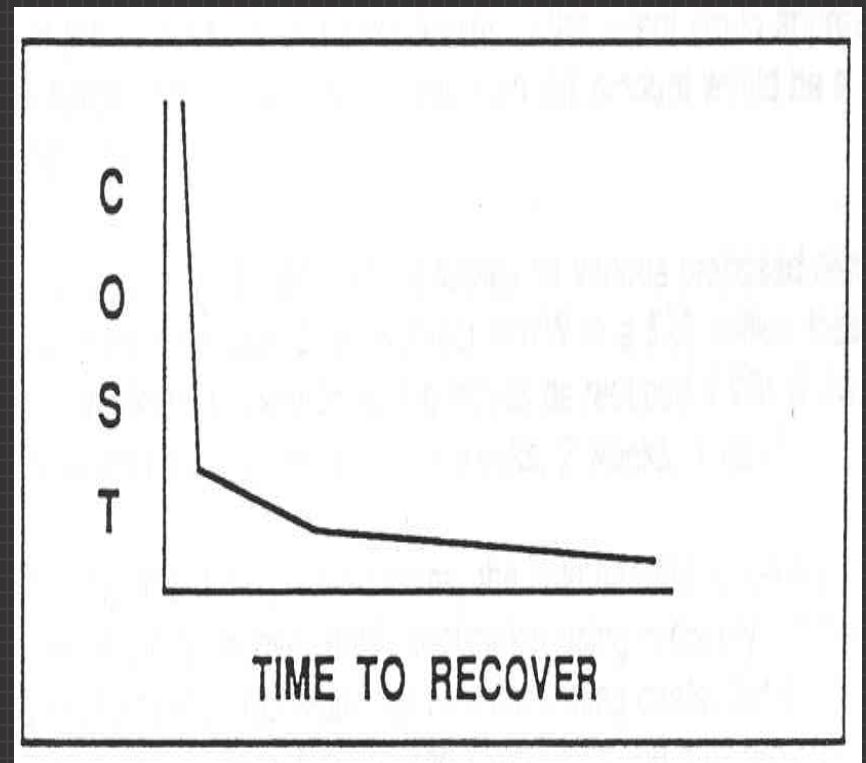
<b>I.</b>	<b>Introduction</b>	<b>1</b>
	Policy Statement	1
	Strategy Overview	1
	Plan Overview and Assumptions	1
	Objective of the Plan	1
	Scope of the Plan	2
	Structure of the Plan	2
<b>II.</b>	<b>Detailed Instructions</b>	<b>3</b>
	Notify Key Personnel	3
	Decide What to Recover	3
	Review the Options	3
	Alternative Sites	3
	Alternative Computer Configurations	3
	Alternative Data Communication Configurations	3
	Notify the Head of Systems	3
	Consult with the Experts	4
	Decide on the Best Alternative	4
	Implement the Alternative	4
<b>III.</b>	<b>Plan Considerations</b>	<b>5</b>
	Choosing an Alternate Site	5
	Choosing an Alternate System	6
	Personal Computers	6
	Output Forms Management	6
	Hardcopy Records	6
	Data Recovery	6
	Personnel Relocations Plans	7
	Required Personnel	7
	Overview	7
	Testing the Plan	7
	Testing Methods	7
	Maintaining the Plan	8
	Maintaining Call Lists	8
	Reviewing Assumptions	9
	Reviewing Requirements	9
	Annual Compliance Reports	9
	Distribution of the Plan	10
<b>IV.</b>	<b>Disaster Recovery Plan Responsibility List</b>	<b>11</b>

## APPENDIXES

APPENDIX A.	Key Library Personnel Notification
APPENDIX B.	Impact Assessment Check List
APPENDIX C.	Alternative Sites
APPENDIX D.	Alternative Computer Configurations
APPENDIX E.	Alternative Data Communication Configurations
APPENDIX F.	Component Level Backup Options
APPENDIX G.	Vendor Contact List
APPENDIX H.	Current Backup Inventory
APPENDIX I.	Current Data Communications Configuration
APPENDIX J.	Current Computer Configuration
APPENDIX K.	Current Computer Room Layout
APPENDIX L.	Emergency Power Support
APPENDIX M.	Emergency Call List
APPENDIX N	Audit Guide

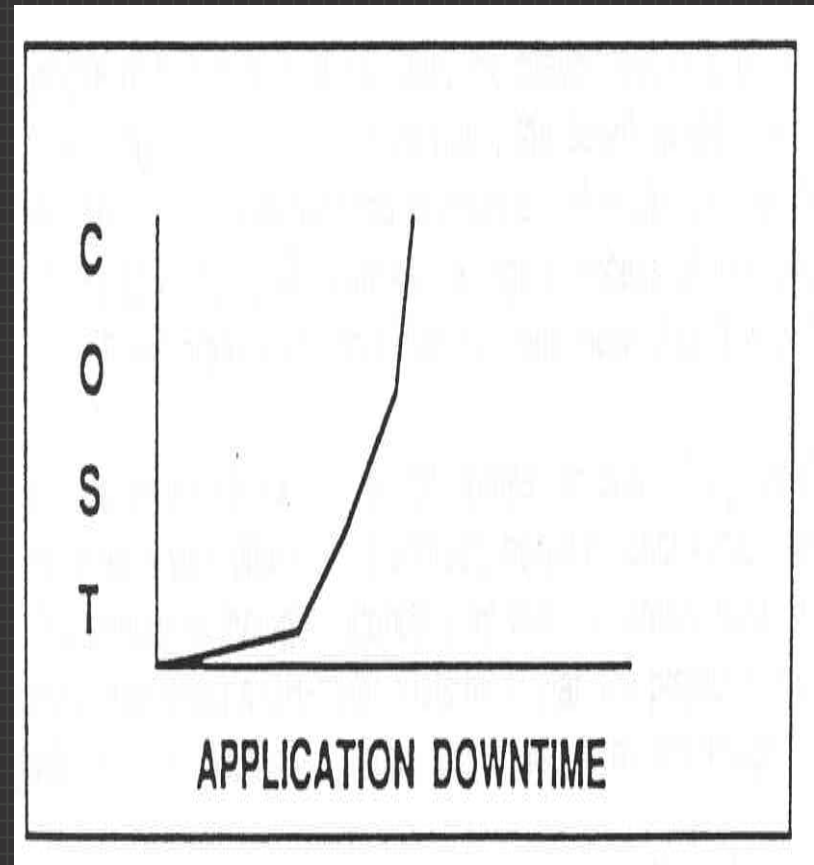
# Window of Recovery

- What is the length of time an application can be down before it negatively affects your organization
- The faster an application needs to be recovered, the more it will probably cost to recovery it



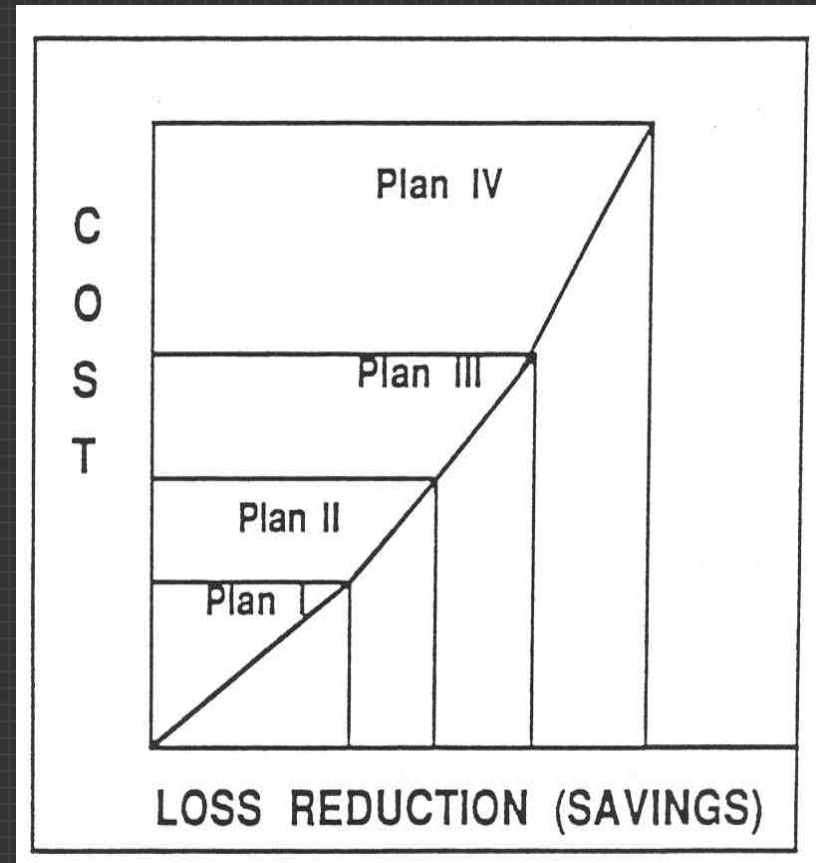
# Cost vs. Application Downtime

- You have to determine how long each business application can be down before the organization loses money, credibility or both.
- What applications need to be recovered and what resources are needed to recover them



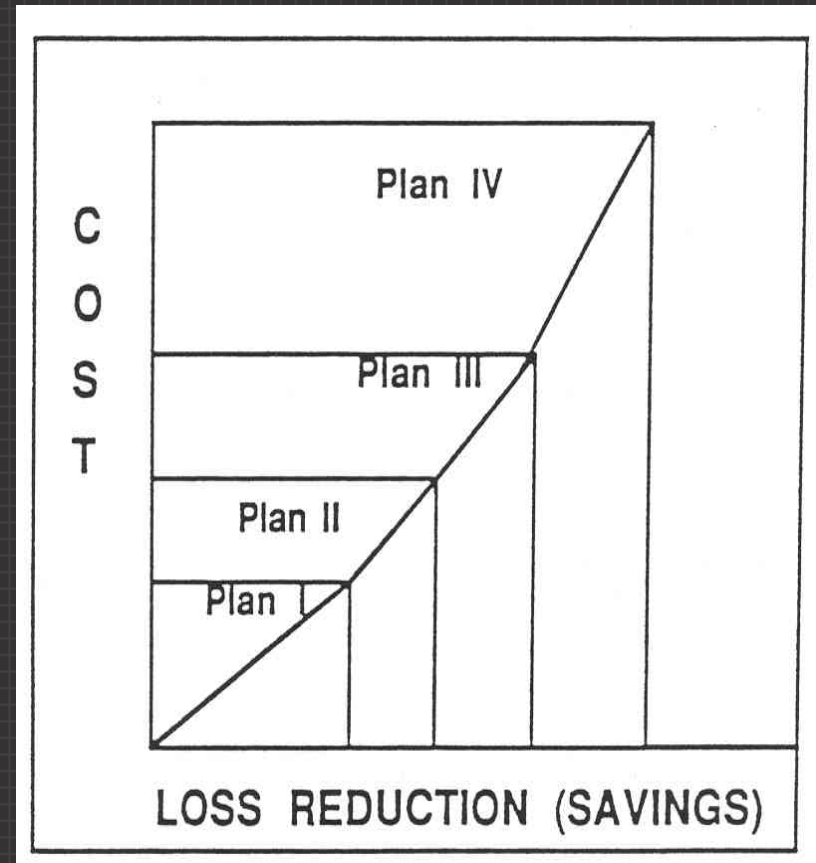
# Consider Alternate Plans

- Without going into detail outline plans
- The time to deploy them
- The associated costs to recover each application using recovery windows



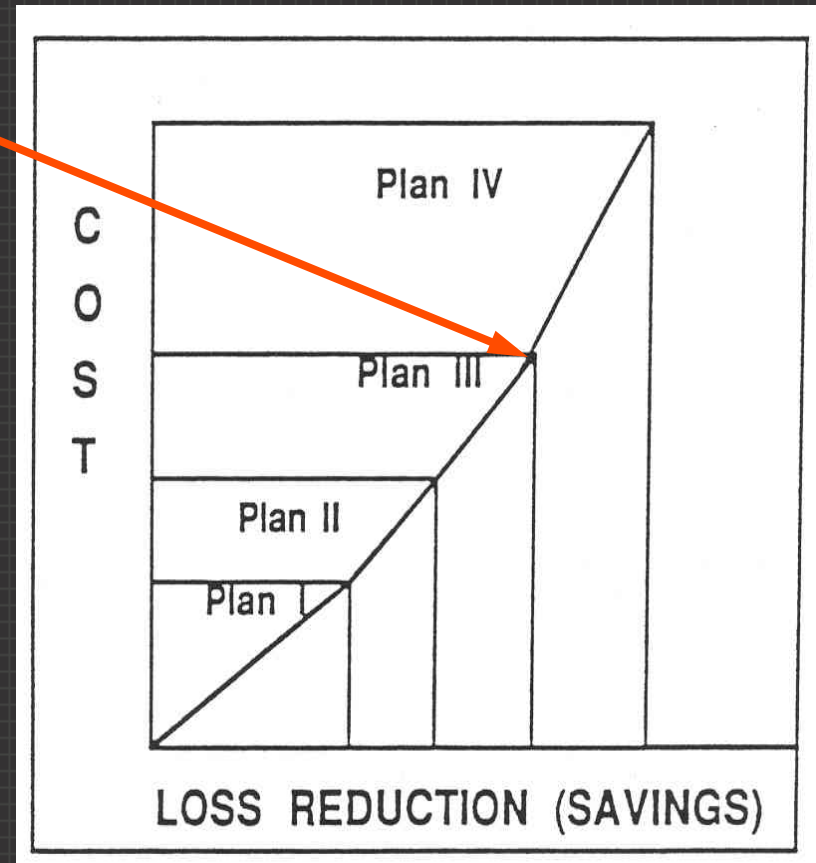
# Consider Costs

- Computing costs
- Alternate sites
- Temporary personnel,
- Hotel
- Meal costs
- Off-site records and forms storage
- Installation of telephones



# Implementation Cost vs. Loss Reduction

- Break Even Point
- Executive staff determine which plan to implement based on cost versus savings and deployment time.



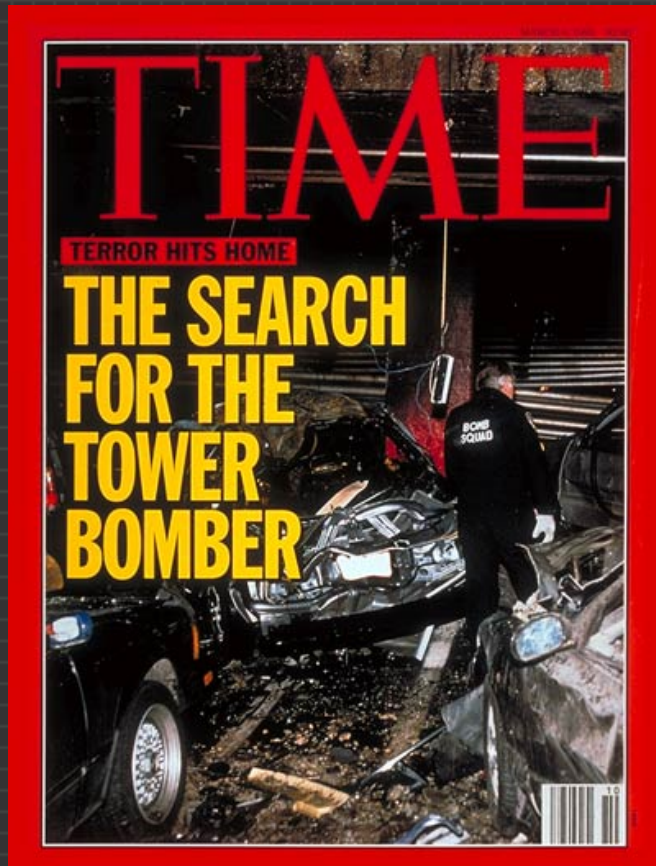
# Primary Risks

- Is the DP Center located in the oldest building the company owns?
- Is it located under the glide path of the local airport?
- Is the organization likely to be the target of terrorists?
- Is it near or on an earthquake fault?

# Secondary Risks

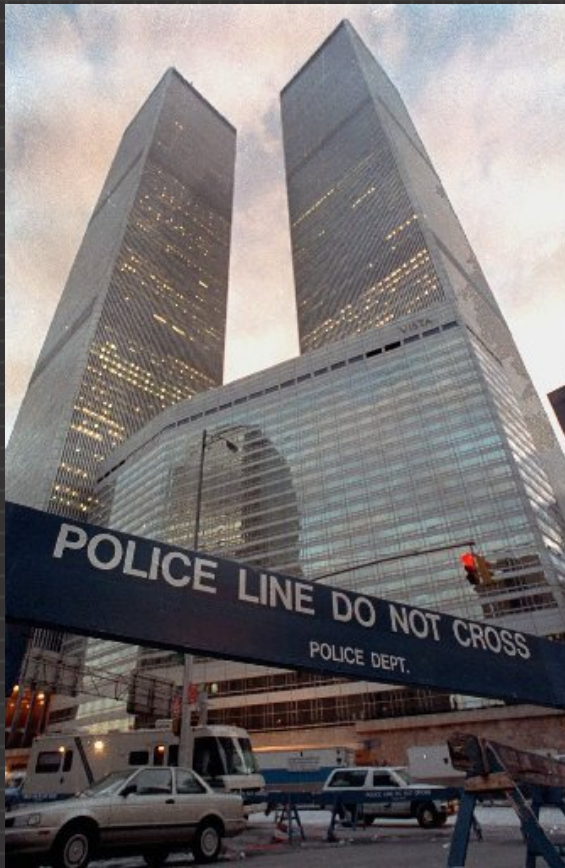
- What would happen to the organization's image if it couldn't recover quickly?
- Would customers go to the competition?
- Would employees leave if they weren't paid for a month?

# 1993



- New York
- Trillion \$ a day
- 80% no DR plan
- Terrorists bombed Trade Center
- 30 days no access
- Where is the backups?

# Lessons Learned - 1993



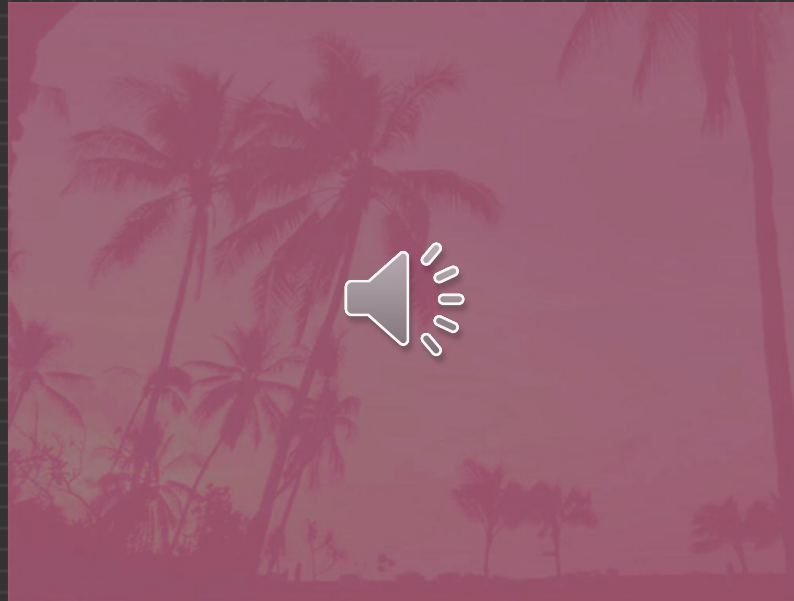
- Back up PCs and store offsite along with central server data
- Don't store data in the same building or close by
- Fail over site

# Lessons Learned - 2001



- Fail over sites worked.
- A few tried to go back in the towers to retrieve data after attack
- Management took BCP seriously

*“I Hate to Alarm You But...”*



“...the computer room is gone?”



October 30, 2004

# 4 Days Up and Running

## **Disaster Recovery Plan**

Recovery and Continuation  
of Automated Library Functions  
at Univeristy of Hawaii at Manoa Libraries



**Systems Office**  
University of Hawaii at Manoa Libraries

- Recover Data
- Fly in hardware
- Establish a network
- Get the cold site functional
- Restore system to the point of failure
- Maintain for 6 years

# 6 Years to Total Recovery

## **Disaster Recovery Plan**

Recovery and Continuation  
of Automated Library Functions  
at University of Hawaii at Manoa Libraries



**Systems Office**  
University of Hawaii at Manoa Libraries

- Selected new data center 2<sup>nd</sup> floor
- Planned and constructed
- Moved servers and services from cold site to new data center in 2010

# Steps to Creating a Disaster Recovery Plan



- ⇒ Phase 1 – Develop the Budget
- ⇒ Phase 2 – Consider the Issues
- ⇒ Phase 3 – Create the Procedure
- ⇒ Phase 4 – Test the Procedure
- ⇒ Phase 5 – Keep Pace With Changes



# Cost-Justifying

Cost-justifying a disaster recovery program is relatively simple.

“No organization can afford to be without one.”

Here are some things to consider.

# Current Cost of Downtime



- Look at both the total cost per minute and cost per event.

- Don't forget to include the intangible or "soft-dollar" costs such as loss productivity and diminished customer confidence.



# Current Cost of Downtime

$$\frac{100 \text{ employees} \times \$14,000 \text{ (salary)}}{220 \text{ days}} = \$6,364/\text{day}$$

$$\$6,364 \times 10 \text{ working days} = \$63,600$$

# Current Cost of Downtime

$$\frac{\$400,000,000 \text{ annual sales}}{220 \text{ days}} = \$1,818,180/\text{sales lost each day}$$

$$\$1,818,180 \times 5 \text{ working days} = \$9,090,900$$

$$\frac{\$9,090,900}{2} = \$4,545,450 \text{ in actual sales lost}$$

# Current Cost of Downtime

$$\$63,600 \text{ labor} + \$4,545,450 = \$4,609,050$$

- ❖ Does not take into account the lost productivity of workers in warehouse, shipping, or in other parts of the organization or external to the organization
- ❖ Does not take into account contractual obligations
- ❖ Does not take into account legal commitments which could result in fines and law suits in the event of malperformance

# Current Cost of Re-Creating Data



- ❖ Consider the time lost re-creating files
- ❖ Expense of retrieving data from storage failure
- ❖ Cost of not having data available when needed
- ❖ Additional support costs involved

# Employing Expert Assistance



- ❖ Compared to the costs of downtime, the costs of hiring the best available expertise to assist with the disaster recover program are trivial
- ❖ Accept estimates from those with core competencies at every aspect of preventing downtime and implementing BCP.

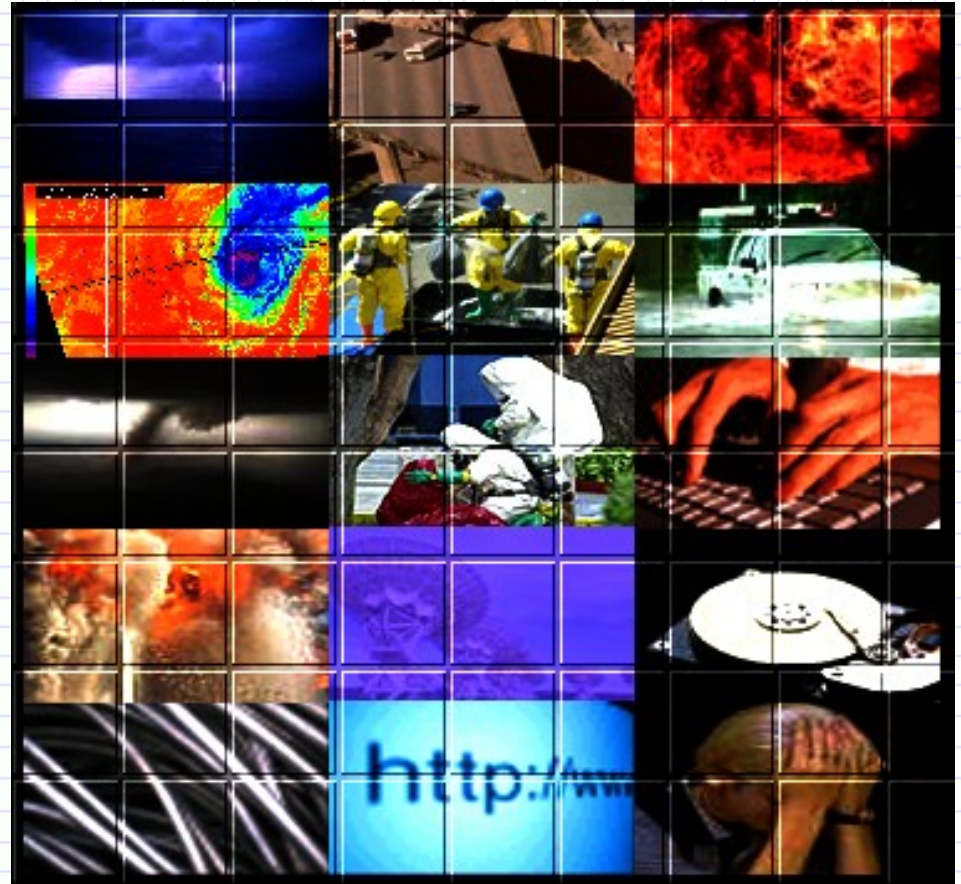
# Consider the Issues

Creating the actual plan is a detailed task that will vary greatly from one organization to another. You should have an understanding of the issues involved.



# What is the Greatest Risk?

- Is your organization more susceptible to natural events such as earthquakes, floods, and tornadoes, fires. Or viruses, intrusion, hackers, human error or terrorism.



# How is Your Organization Affected By Downtime?

- For each department, how vital is access to data?
- How long could department function without access to the data they need.



# What Preventative Measures Are In Place Now?

- Is there a disaster team?
- What is the backup strategy?
- Where is the backup stored?
- Are things documented?



# What Preventative Measures Are In Place Now?

- Do you have redundancy in place, such as backup data communication lines?
- Who is in charge of managing the recovery effort.
- What happens if key personnel can't respond to a disaster?



# Keep Pace With Changes

- Change is the order of the universe
- Your plan must be reviewed, and possibly updated when changes in the organization take place: personnel, new departments, facilities.

## **Disaster Recovery Plan**

Recovery and Continuation  
of Automated Library Functions  
at University of Hawaii at Manoa Libraries



Systems Office  
University of Hawaii at Manoa Libraries

# The Plan Review

- Is there an ongoing review of the plan?
- Who maintains the logistics and names of the disaster management team?
- Are changes to the plan communicated to those affected?

## **Disaster Recovery Plan**

Recovery and Continuation  
of Automated Library Functions  
at University of Hawaii at Manoa Libraries



Systems Office  
University of Hawaii at Manoa Libraries

# The Plan Review

- Consider how your organization, the state and FEMA will work together if warranted to resolve issues
- Build reporting elements into data sets to expedite claims to all of these agencies.

## **Disaster Recovery Plan**

Recovery and Continuation  
of Automated Library Functions  
at University of Hawaii at Manoa Libraries



Systems Office  
University of Hawaii at Manoa Libraries

# Further Information

- Disaster Recovery Journal
- <http://www.drj.com>
  
- The Business Continuity Journal
- [businesscontinuityjournal.com/](http://businesscontinuityjournal.com/)



# Questions?



UNIVERSITY *of* HAWAI'I®  

---

MĀNOA

James Paul Adamson  
adamson@hawaii.edu