
Computer Disaster Recovery Plan (CDRP)

Treat Computer Disaster Recovery Plan (CDRP) as your Insurance to your mission critical business!

Companies can be quite cautious when it comes to protecting themselves against financial and physical risks. Many would regard actions such as fire insurance for their premises, hedging against currency fluctuations, and round-the-clock security for their plants, as routine precautions against potential threats to their business. And it is true that these things happen regularly.

However, many companies seem less vigilant when it comes to protecting their ability to continue doing business if they are ever hit by certain types of disasters - the kind of catastrophes that can put them out of business totally are also the ones that have the least of chance of occurring.

But what if a disaster did occur?

For many organizations, investing in a system that will help back up critical business data is like buying life insurance - it is always a safe choice and should prove to be beneficial later. Organizations must draw up a disaster recovery plan, identify operations which are critical to their business' survival, and assign staff to handle the tasks needed to get their business up and running again as soon as possible after a major catastrophe.

At Sapura Synergy – managed services unit, we help you to save time, resources and costs by outsourcing your computer disaster recovery needs to us. Our objective is to provide for the timely availability of all resources that are necessary to operate critical business processes at a level acceptable to senior management. The key here is maintaining timely availability, and not just reacting to disasters. Case in point, a bank - this would mean being able to continue providing the more critical services, such as deposits and withdrawals, to customers within a reasonable period of time after being hit by a particular disaster.

To understand computer disaster recovery plan, a good understanding of the term disaster and the types of disaster occurring is important.

DEFINITION OF DISASTER

Disaster can arise inside or outside of the organization regardless of the prevention techniques employed. Potential exposures may be classified as natural, technical or human threats.

Catagories of Disasters	Definition of Catagories of Disasters
<p>Technical threats</p> <ul style="list-style-type: none"> Hardware or system malfunction accounts for 44% of possibility data loss Software corruption or program malfunction accounts for 14% of possibility data loss Computer viruses accounts for 7% of possibility data loss <p>Human threats</p> <ul style="list-style-type: none"> Any form of human error acts accounts for 32% of possibility data loss <p>Natural threats</p> <ul style="list-style-type: none"> Any form of natural disasters accounts for 3% of possibility data loss 	<p>1. Technical Threats : power failure / fluctuation, heating, ventilation or air conditioning failure, malfunction or failure of CPU, failure of system software, failure of application software, telecommunications failure, gas leaks, communications failure, nuclear fallout.</p> <p>2. Human Threats : robbery, bomb threats, embezzlement, extortion, burglary, vandalism, terrorism, civil disorder, chemical spill, sabotage, explosion, war, biological contamination, radiation contamination, hazardous waste, vehicle crash, airport proximity, work stoppage (Internal/External), computer crime.</p> <p>3. Natural Threats : internal flooding, external flooding, internal fire, external fire, seismic activity, high winds, snow and ice storms, volcanic eruption, tornado, hurricane, epidemic, tidal wave, typhoon.</p>

THE NEED OF COMPUTER DISASTER RECOVER PLAN

Disaster Recovery Plans & Systems Are Essential. Two out of five enterprises that experience a disaster such as World Trade Center Attack go out of business within 5 years. Business continuity plans and disaster recovery services are important to ensure continuing viability.

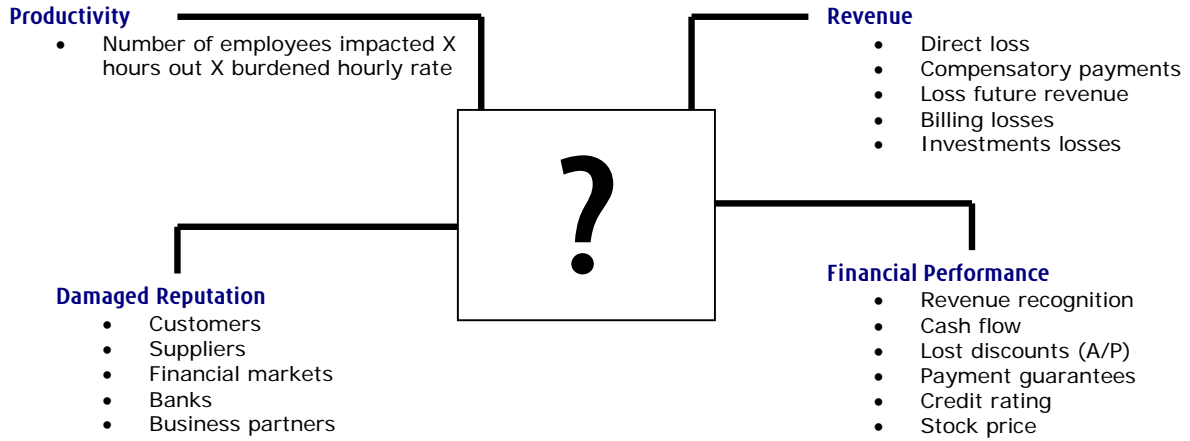
According to research firm, International Data Corporation (IDC), "Duplicating data is growing more prevalent. Makers of backup and recovery software booked US\$2.7 billion in revenues last year, and that figure is expected to grow to US\$4.7 billion in 2005". Sources: Contingency Planning Research & Strategic Research Corporation.

The statistics reveal:

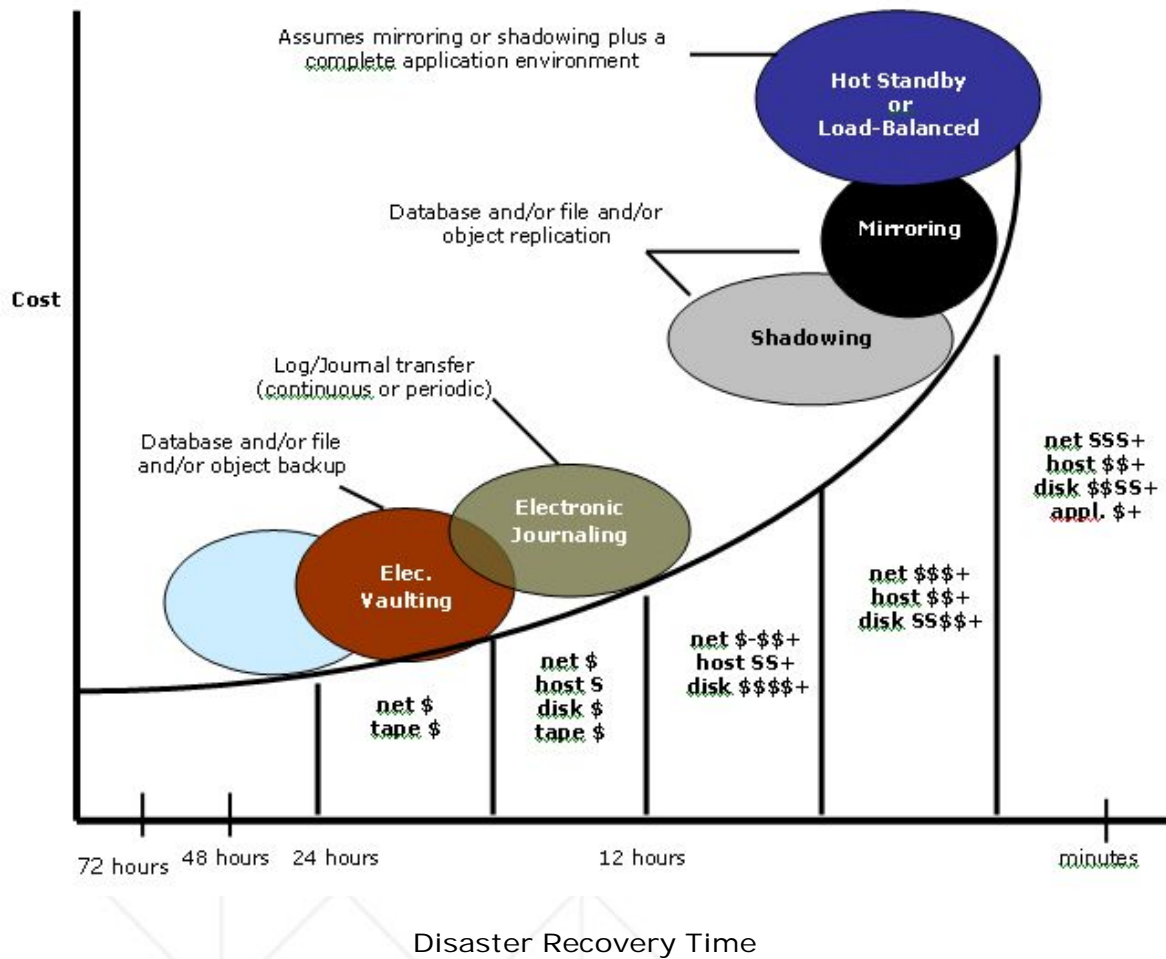
Possibility of Data Loss	Cost of Data Loss (Based on Average Hourly Impact)	At what point of downtime is the survival of your company at the risk?
Hardware or System Malfunction	44%	Retail Brokerage USD 6.5 million
Human Error	32%	Credit Card Sales USD 2.6 million
Software Corruption or Program Malfunction	14%	Authorization USD 110,000
Computer Viruses	7%	Home Shopping Channels USD 90,000
Natural Disasters	3%	Airline Reservation Centre USD 28,250
		Package Shipping Service USD 26,761
		Manufacturing Industry USD 17,093
		Banking Industry USD 9,435
		Transportation Industry USD 9,435
		Within the first hour 4%
		1 hour 3%
		4 hours 9%
		8 hours 8%
		24 hours 15%
		48 hours 21%
		72 hours 40%

Sources: Contingency Planning Research & Strategic Research Corporation

WHY CDRP?



What is YOUR COST of downtime?



Computer Disaster Recovery Plan (CDRP) Packages

We offer 4 packages of CDRP . The packages are :

- Cold-Site
- Warm-site w Shared Servers
- Warm-site w Dedicated Servers
- Hot-site

Packages Model :

Description	Cold-Site	Warm-site w Shared Servers	Warm-site w Dedicated Servers	Hot-site
D1's part of Turn-around Time	6 Hours	6 Hours	6 Hours	6 Hours
Hardware / Infrastructure Investment				
Servers	-	NT / Solaris shared among 3 customers (DIFF customer are > 5km apart)	x2 servers in Primary sites	x2 servers in Primary sites
External HDD	-	Optional Dedicated HDD	-	-
Space	Dedicated Rack Space, ready for occupation	Servers sits on Rack Space assigned, server non-activated		-
Parameters Provisioning	Pre-assigned IP addresses			Pre-assigned IP addresses
Data Center Facilities	Full Data Centre Facilities (Fire Suppression etc...)			
Data Backup	Either: 1. Customer to manage their own Data Backup system 2. Subscribe to DataOne's Backup system			Mirroring / Regular Patching
Leased Line	-	-	-	Optional for mirroring / patching
Manpower During Disaster				
Hardware Readiness	Coordinated delivery with vendor	-	-	-
OS Readiness	Coordinated delivery with vendor / Install upon startup	-	-	-
Application Readiness	Provide & installed by customer	Provide & installed by customer	-	-
Data Readiness	Customer to recover from Backup (unless customer is on D1 backup plan)	Customer to recover from Backup (unless customer is on D1 backup plan)	Customer to recover from Backup (unless customer is on D1 backup plan)	-
IP / DNS Readiness	-	-	-	DNS Configuration done by customer

Computer Disaster Recovery Plan (CDRP) Packages

Manpower During Normal Mode				
Hardware Readiness	-	Monthly Hardware testing	Monthly Hardware testing	System Live
OS Readiness	-	Ensure OS installed with patched	Ensure OS installed with patched	OS Live
Application Readiness	-	Customer to ensure that applications are available to install when needed	Customer to ensure that applications and patches	Application Live
Data Readiness	-	Advise customer do backup of data	Advise customer do backup of data	Frequent mirroring or patching
Rehearsal	-	Yearly test of up to 3 days	6-monthly test of up to 3 days	Customer can do rehearsal anytime

Common Options	
Office Space	<ol style="list-style-type: none"> 1. FM Room (max capacity 10pax) 2. Conference Room (max capacity 16pax) 3. Meeting Room (max capacity 6pax) 4. 3rd Floor Office Room (max capacity 10pax with cubicles) Network-ready cubicles for ops staff / designer rooms for command center with remote console access.
Office Equipment	<ol style="list-style-type: none"> 1. Analog Phone 2. Facsimile Machine (Std) 3. Photocopier 4. Whiteboard 5. Laptop (Win 2000 with MS Offices)
IT Consultancy	IT Consultancy on the Disaster Recovery System – System Implementation Review
Optional Parameters	<ol style="list-style-type: none"> 1. Domain Name Hosting (Primary / Secondary) 2. Internet Bandwidth (increase from 64kbs)
Documentations	<ol style="list-style-type: none"> 1. SOP 2. Reports after Rehearsals (twice yearly) 3. Reports after Recovery