

# From the Catwalk

...our take on current trends in technology

## Disaster Recovery In The Post-911 Economy

The subject of the necessity of a business continuity plan is something that's on everyone's mind. Is it something you need for your organization?

Think about this: while the overall spending for technology may be down from past years, CIOs at companies large *and* small agree that the one critical area of technology spending and emphasis for this year is the combined security and disaster planning. Here's the Catwalk Perspective on what is most important in developing your company's Disaster Recovery plan (DRP).



## What is a DRP?

First let's define what we're talking about.

A reliable DRP details the specific steps, protocols and procedures that a company should have in place (with respect to the technical aspects and functions of a business) before, during and after a disaster occurs. We've found that while many companies have some sort of data recovery plan, it's more like an untested concept referring to loss of data. The majority of organizations have not gone to the next level and created a more **comprehensive business continuity plan**.

Second, let's realize that a plan is only as good as it's implementation.

In the case of an effective DRP, it must be more than an email to senior management or a document that sits on your IT Manager's desk. The most effective DRPs start with **tasking the right internal team** of people with the plan's development. Once developed, an extremely effective team leader keeps the plan alive. This person is someone who meets five criteria:



1. shows a solid understanding of your business
2. exhibits unrivaled project management skills
3. demonstrates thorough understanding of the specific technical resources needed for the plan's overall success
4. communicates effectively up, down and across your organization
5. devotes the ongoing amount of time needed to give the DRP a successful outcome

## What Should The Plan Include?

Basically a functioning DRP has four components.

To start, an effective DRP includes not only the steps to implement if a disaster strikes, but also definitions of kinds of events and what would need to be done for each. To be most effective, create a list of the **likely scenarios and situations** that may affect your business. The list would include

- § Natural disasters
- § Unintentional system error (computer or human)
- § Malicious attack on your system (from internal or external sources)

Then go back and list out those events that you would have considered unlikely just five months ago. Consider the scenarios for those and what steps need to be in place to keep business going or be able to start business back up in **very short order**. Among the items on this list might be:

- § Kidnappings
- § Hijackings
- § Robbery/Theft
- § Explosions
- § Extended loss of power

By the way, in case you think this might be an exercise in overkill, **consider this fact:** so many of the companies victimized by the attack on the World Trade Center were able to get past their devastating losses and begin to conduct business in short order because they had effective DRPs that stemmed from the World Trade Center bombing in the mid-90s.



When creating your scenarios, be sure to keep in mind events that may indirectly have an effect on your business, i.e.: a problem for partners, vendors, suppliers or, even, customers.

Next, determine what **functions** are critical in your day-to-day business. Ask yourself these two questions:

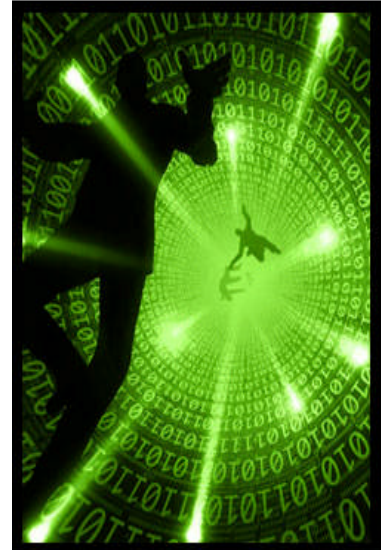
- § What would we do if disaster struck today?
- § What processes are currently in-house or in place with vendors, partners and suppliers that will help your business recover?

Then, **look for the holes**.

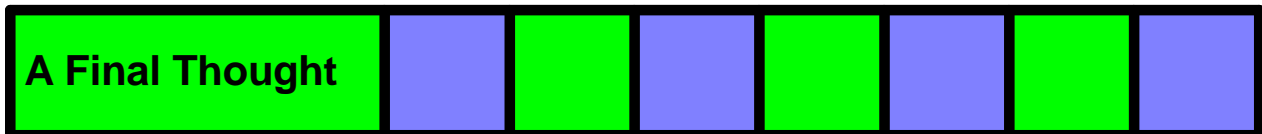
Develop contingencies that fill the holes, keeping in mind the following:

- § What triggers the plan?
  - Be sure to define the chain of events that set your DRP in motion
  - Make sure the communication hierarchy is mapped out and appropriate

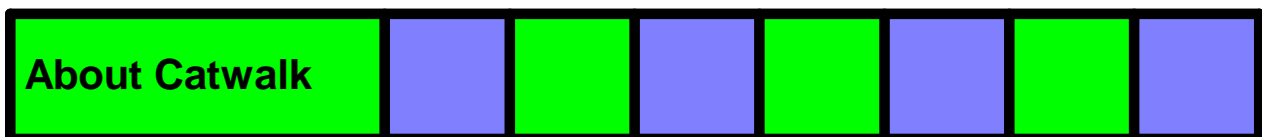
- § Who manages the plan?
  - Be sure each leader is aware of the details of the plan that effect that arena
  - Make provisions for back up
    - § Be sure to cover all bases in case key or assigned personnel aren't available
- § What resources are involved?
  - Can you tap resources at alternate locations once the plan is activated?
    - § Be sure to look at the threats to their viability
  - What relationships do you need to establish and maintain with providers of contract resources?
- § Does the PLAN work?
  - In other words, have the backup systems been tested?
    - § Remember your backups are only as good as their ability to function in time of a crisis
- § Will your staff execute the plan?
  - Are they trained as needed?
  - Do they believe in the plan?



Finally, as with any plan, **it's only as good as it's functionality.** It must be reviewed and revised on an ongoing basis (we recommend quarterly) to be effective.



If you're wondering whether or not a DRP is just one more sounding of an unnecessary alarm for you business, consider that tech researcher Gartner estimates that two out of every five enterprises that experience a disaster will go out of business within five years. Those with DRPs have the abilities to improve those odds.



Catwalk Consulting is known for providing clients with a different perspective to the link between business and technology. For more information about the specific information in the tech trend or to talk with us about your business and technology needs, contact us, at [info@catwalkconsulting.com](mailto:info@catwalkconsulting.com) or call at (888) 989-0196.

Know someone who should receive our tech trends? Send us their e-mail and we'll buy you a cup of coffee. Is there a topic you interested in hearing more about? Let us know and we'll put the Catwalk team to the task.

To be removed for our mailing list, email us at [info@catwalkconsulting.com](mailto:info@catwalkconsulting.com) with "Remove" in the subject line.



Copyright 2007 - Catwalk Consulting. All rights reserved.