Modeling Events
To
Affect a Recovery

How do you begin planning specific recovery strategies for a disaster event that hasn't happened yet? Industry best practices and your own good sense suggest that you use the worst-case scenario to determine the necessary recovery strategy to be used. It follows, that if you can account for all elements of a recovery from the worst-case event, you could use the appropriate sub-set of tasks to recover from the less-than-worst-case event – which, of course, is more likely to happen.

Since 9/11 the case for worst-case planning has become stronger, but does not address those recovery steps, tasks and procedures that need to be taken for a less than worst-case event.

Consider that in order to recover a business unit and its functions you would take different steps if the building were leveled by a tornado than if the data center that supports the computer applications were to become inoperative for 48 hours. Recovering from worst-case requires that you consider all recovery elements and all steps, tasks and procedures necessary to regain functionality. The data center inoperability scenario requires only those steps, tasks and procedures to connect to a hot site for processing continuation after the IT recovery team has restored critical applications. For business unit personnel, this may mean continuing in a manual mode until connectivity with the hot site is made but would not require that they implement moving the unit to an alternate site.

Not only does the worst-case event seldom occur, but when it does, the event will probably take a form unplanned for by the best and most far reaching recovery plan and you will end up scrambling for an ad hoc strategy to meet the circumstances. In any event, you must go through the worst-case recovery steps, tasks and procedures in order to find the set of actions to take for the disaster event at hand whether it has happened to the data center, the building in which the business unit is housed or in some other fashion has rendered the business unit unable to complete its critical processes.

What does it take, then, to prepare not only for a worst-case event but for less severe events that are likely to occur in some way requiring you to be creative in applying a recovery strategy?

The answer is that it takes consideration of **two** important elements of an alternate way of planning for recovery:

- A model of events that will allow you to pinpoint the type of event that you are dealing with and that also suggests a strategy or set of strategies that will best provide for recovery. This model, to be of value, must include both event type and event severity. It must also contain specific risks and threats to your organization so as to provide assistance to the management team charged with disaster declaration and event management.

- Realistic Recovery Strategies for each identified critical process or function that can be documented in recovery plans and can be executed by the existing recovery teams. These strategies come from the risks identified for the organization and will span a gamut of actions from "Stand-By for further instructions" to "Relocate to an alternate facility". It must also include a time line that allows for movement from an immediate set of actions to a more strategic longer term set of recovery actions as time from the onset of the event passes. More discussion of this element appears below.

What Constitutes an Emergency Event?

An emergency event can happen to computer systems, facilities or personnel; individually or in combination.

- A computer virus brings down critical IT applications
- A facility is hit by a tornado
- An overnight flood or snow storm prevents critical personnel from getting to their place of business
- The tornado heavily damages the facility housing the IT department and the equipment running critical applications

These examples can provide for a localized, low level of severity as well as a catastrophic, high level of severity. What might start out as a facility event, a localized fire in the telephone closet perhaps, may accelerate to a severe facilities event that has rendered the data center uninhabitable and inoperative after four hours. The following elements of a disaster event must be accounted for in any model that would prescribe an appropriate response strategy.

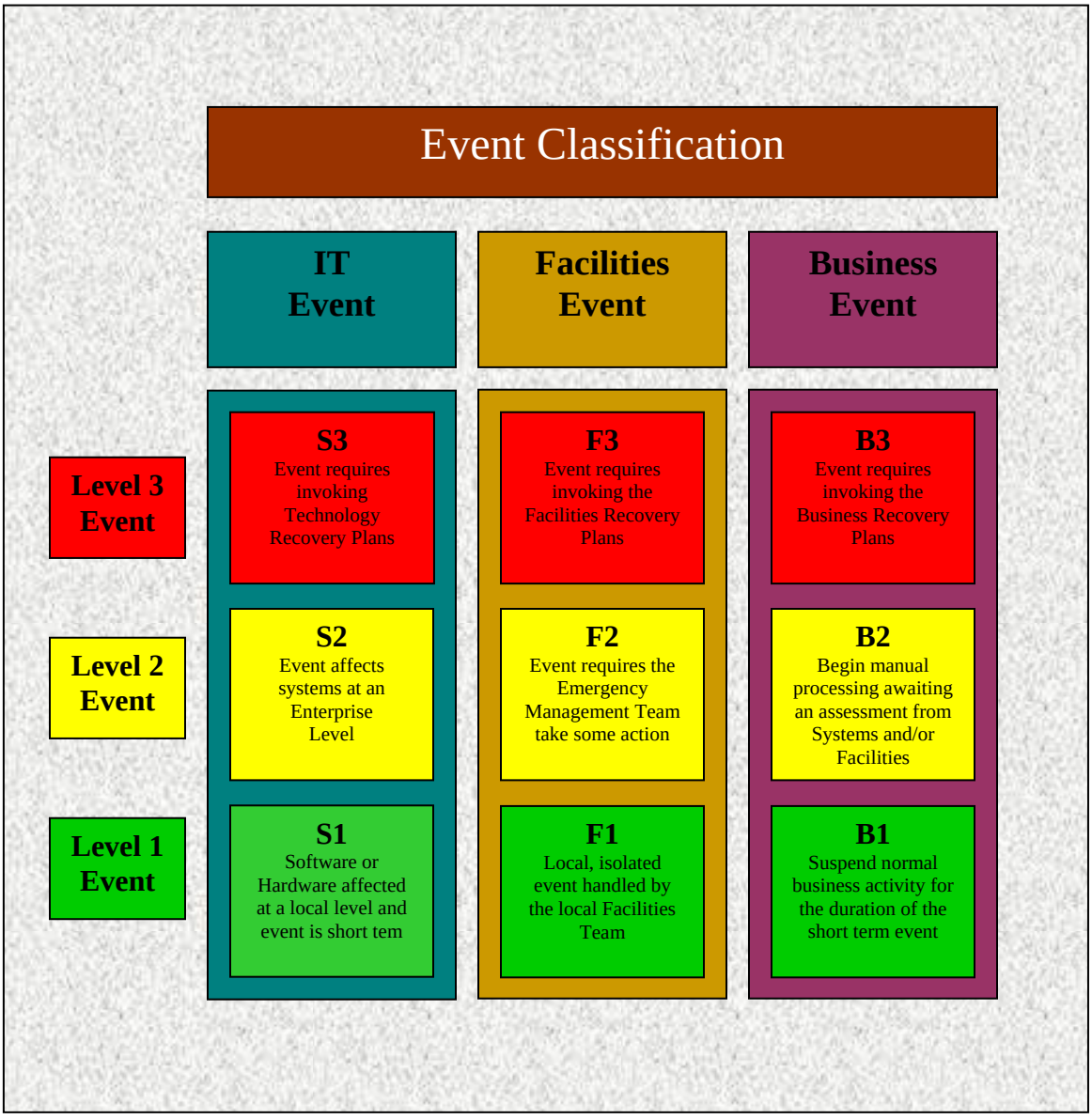
- The object of the event (facility, IT component(s) or business unit personnel)
- The level of severity, and
- The time since the onset of the event

What does an Event Model look like?

The following chart provides a generic model of events that will be used to illustrate the factors impacting recovery. Although three levels of severity are depicted here, it is an arbitrary number. The important distinction to make is that different activities should be prescribed for different levels. If the actions to mitigate the risks and threats discovered in an assessment phase of recovery planning are best described in 4 or 5 levels of severity, then the model for your organization should provide for each.

Type and severity are abbreviated in the following discussion as:

- **S1** – Level 1, IT event
- **F2** – Level 2, Facilities event
- **B3** – Level 3, Business event



Specific applications, facilities or critical business functions described in each silo for each level and matching the risks and threats to the organization will bring the applicability of the model into focus and will provide a standard starting point for the emergency management team to apply to the event.

Level 1

A level 1 event is local in nature and does not require escalation outside of the affected area for resolution.

Level 2

A level 2 event would most likely be an escalation of a level 1 event and would require support from outside the local area for resolution. Invocation of some part of the appropriate recovery plans may be necessary.

Level 3

A level 3 event would most likely be an escalation of a level 2 event or a reaction to a severe event. In addition, a level 3 event will most likely affect an entire facility, data center, or business unit. Recovery plans will be activated for level 3 events and would require coordination among IT, Facilities, and Business Partners.

Note that escalation from one level to another can occur over a short period of time or can be instantaneous.

Describing the Appropriate Recovery Strategy

Once the emergency management team has determined the type and level of severity of the event, the statement in the appropriate box probably will not give enough guidance to begin recovery. What is needed is to translate the level and event type into an appropriate recovery strategy selected from a full set of possible strategies.

If we have determined that there has been an S2 event, we will need a place in all recovery plans for a straightforward representation of what recovery steps should be taken at the onset of the event (0-48 hours) and, if the event continues, what steps to take until the event is resolved and the recovery is made (hours, days or weeks).

The following table can serve as an example containing all appropriate recovery strategies for each level of severity (represented vertically) at each critical period of time from the onset of an event (represented horizontally). Please refer to the Table Key below for a description of each recovery strategy applied in this example.

Severity	Sample Recovery Strategy Table				
S3	S/MP	AS/MP	AS/MP/BL	AS/MP/BL/RTN	AS/MP/BL/RTN
F3	S/MP	AS/MP	AS/MP/BL	AS/MP/BL/RTN	AS/MP/BL/RTN
B3	S/MP	AS/MP	AS/MP/BL	MP/BL/RTN	MP/BL/RTN
S2	S/MP	MP/BL	MP/BL/RTN		
F2	S/MP	MP/BL	MP/BL/RTN		
B2	S/MP	MP/BL	MP/BL/RTN		
S1	S/MP				
F1	S/MP				
B1	S/MP				
RTOs	**0 – 48 hrs**	**48 – 72 hrs**	**72 – 96 hrs**	**5 days**	**2 weeks**

Table Key:

S = Defer Action/Stand By: Normal activity is suspended and recovery strategy delayed. Awaiting further instructions.

MP = Manual Procedures: Manual workarounds for recovery of critical business processes.

DP = Distributed Processing: Critical processes are performed at geographically dispersed sites not affected by the event.

BL = Backlog: Teams work the accumulated critical tasks that have been backlogged.

RA = Reciprocal Action: Prearranged agreements to shift critical business processes to an unaffected party (internal and/or external).

AS = Alternate Site: The unit must move its entire operation to a predetermined alternate location.

ALT = Alternate Source: Use of an alternate provider of a product or service when the primary source is affected by an event. This strategy is for readily available, non-specialized products or services.

I = Idle. Unit processes (non-critical) cannot be performed and unit personnel are available to assist in the recovery of other critical units and processes.

RTN = Return to normal operations (either at an alternate site or upon returning to the home site).

RTH = Return to home.

Business units with more than one critical process to be recovered may need a different strategy for each at any given point in the event. The S2 event used as an example above may require the “Stand By” recovery strategy for data entry via a terminal device, while another critical process of the same unit – answering the customer phone calls and questions - may continue with a workaround strategy of “Manual Procedures” and be kept for input after the event is over and the applications systems that support the data entry and collection of statistics is available for use.

How to Organize a Recovery Plan

Using this methodology to determine the appropriate recovery actions to take requires that the rest of the recovery plan be organized according to critical process. A statement of each critical process, that is, the core unit activity that must be completed for the unit's mission to be successful, should be followed by the steps, tasks and procedures associated with each recovery strategy applicable to its recovery. Manual procedures and working the backlog may be identical for each process and can be pasted after each critical process statement.

For example, one of the unit's critical processes is:

Provide timely telephone support to customers calling to add, change or delete information from their records

In order to successfully complete this process, the unit members must be able to call up the correct customer record or create a new customer record from an online database and interact with the customer and the information displayed. The application system providing this online information display also keeps track of demographic data and when something is changed, a report is generated for use by another unit within the company.

Using our sample strategy table above, the immediate strategy for the unit personnel responsible for this process is to 'Stand-by' and, if necessary, perform some predetermined 'Manual Processes'. As the event continues into a second or third day, the strategy changes to one of performing manual processes and working the backlog of transactions. It may be that after day two the event escalates to an S3 level at which time the unit performs its predetermined steps and tasks to move operations to an alternate site (with connectivity to the IT hot site).

In this limited scenario the critical process of providing phone support is identified in the recovery plan and is followed by the appropriate steps, tasks and procedures for each applicable recovery strategy: Stand-by, Manual Processes and Alternate Site. This format is to be followed for each critical process identified for the each unit. In this way, the plans for all units are formatted the same, and if reorganization or unit mission changes critical processes from one unit to another, update and maintenance of each recovery plan is accomplished by removing the critical process and its attendant recovery strategies from one plan and placing them in the other.

Just Another Way to Complicate Planning?

The reader may consider the methodology described here as a more complex and complicated way of creating a recovery plan. After all, as has been declared early in this article, if the steps and tasks required to recover from the worst-case scenario are documented, the recovery team that is already familiar with the critical processes can surely manage an ad hoc recovery from some lesser event.

Those of us who have gone through recoveries, either of our own or as a service provider in support of a recovery, have at least one common experience – the stress and trauma that accompanies a disaster event comes to bear on every facet of the recovery process. The actual or potential loss of or injury to fellow employees and, in the case of an event occurring in the community as a whole (hurricane or tornado), concern for the safety of ones family will take priority over recovery. Although extreme, recovery teams that have exercised their plans successfully several times have been known to not even refer to the documented plan when a real event happens. The stress and trauma of the event has seemed to render them without focus and they have not known where to start the recovery process without prompting from outside the emergency circumstances.

An event model and table of recovery strategies documented in the recovery plan forces the recovery team to focus on each step of the recovery effort - from identifying or having the type and level of event identified for them, to taking each critical process and focusing on the steps, tasks and procedures required to restore its functionality.

It is felt that this organization of recovery plans and its requirement that members of a recovery team focus on simple, incremental and straightforward recovery processes will greatly assist in making the recovery successful. Put another way, how do you eat the elephant (during a disaster)? The answer, of course, is - one bite at a time (step by step)!

An Event Model, customized to your set of risks and threats, can become the focus at the beginning of a disaster event and can mean the difference between a successful and a less than successful recovery effort.

Garry Bond is the Principal Consultant for Sage Business Associates, Inc., and has been an ACP member since January 2003. He is currently a member of the Colorado Rocky Mountain Chapter of ACP.
He can be reached at:
Office - 303-841-4467

Cell – 720-989-5039
or by email at glbond80134@msn.com.