

Are You Incident READY?

Jim Mitchell, CBCP, Director, eBRP Solutions Inc.

- You have Plans.
- Your Call Trees are updated.
- You have a Crisis Management Team in place – and an EOC to house them.
- You've run tabletop tests and made sure every Plan is up-to-date.
- Your auditors are happy. Senior Management is happy.

But are you really Incident READY?

When the 'moment of truth' arrives, will everyone know what to do? Will decision makers have the information they need to make decisions? Will you be able to coordinate the needs and demands of Recovery Teams and business management? Or will you be forced to 'wing it'?

No two incidents are alike. An incident may cause a disruption to day-to-day operations, but still not be classifiable as a 'disaster'. A 'disaster' may not disrupt everything. Regardless of whether your BCM program relies on Scenario-based Plans or Asset-based Plans there is one guarantee about your next business disruption: you don't know what will happen, when it will happen, how severe it will be or how long it will last.

So how can you be sure you're prepared for the unexpected? What will it take to make certain your organization is Incident Ready?

Managing an Incident

No matter how many plans you have, or how frequently you test them, it's the Incident Management Team (or Crisis Management, Incident Command or whatever you choose to call them) that will be the linchpin of your organization's response efforts. Once the unexpected happens, it's the decision-making of the Management Team that will determine whether the outcome is a success or less than optimal.

Becoming Incident Ready requires that the Management Team have a dependable decision support system at the ready. While others may perform the actual Incident Assessment, the Incident Management Team (IMT) will need additional information to evaluate the Assessment in order to fully understand the Impact. Their decision support system must help decipher the impact across the organization. Not just what happened, but how it is impacted by the day of the month and time of day of the disruption.

Where does that information come from? Certainly a thorough Business Impact Analysis may have surfaced much of it. But are the BIA results in a form and format that will enable a thorough analysis of a specific impact in real time? Has BIA information accounted for the dependencies and interdependencies that must be understood to make strategic decisions?

Organizational Interdependencies

Incident Management requires swift and strategic action. But performing a real-time assessment of the implications of a disruption require access to intelligence; intelligence that spans the entire organization. The same type of "what if?" analysis that can be useful in creating recovery planning strategies must be deployable in an actual disruption.

No business unit or function operates in a vacuum. Every organization, regardless of size or scope, is a virtual spider web of interdependent activities. An impact on one function has a ripple effect across the organization. In order for the IMT to invoke appropriate response Plans, it must have an understanding of both the direct impact of the disruption and the indirect impact resulting from the interdependencies of the impacted functions. Without that knowledge, taking action is similar to a doctor treating the symptoms, rather than the underlying disease.

Once the full impact of a disruption – including the impact on dependent processes and functions – is understood, the IMT can begin to take effective action.

Establishing Operational Command

Many organizations establish Emergency Operations Centers in advance. Stocked with phones and computers and copies of BCM documents, these EOC's are intended to provide an IMT command post in the event of a disruption. But often, all the planning effort goes into communication devices, and too little advance planning goes into what tools the IMT will need to effectively take and maintain control of the flow of activities.

The role of the IMT is three-fold: Command, Control and Communication.

Command

Planned properly, the Command role of the IMT should be understood by all employees (and especially those charged with executing recovery Plans). A business disruption is not the time for independent action. Recovery teams must constantly be aware that their actions and activities are tightly intertwined with the activities of other teams. The IMT must have both the mandate and the ability to monitor and manage the activities of recovery teams – sometimes dozens, or even hundreds of teams.

Control

Having assessed the impact and decided on recovery strategies, the IMT must possess the information necessary to maintain control of the flow of activities. They must understand what resources (people, facilities, technology, equipment, and process capabilities) are available, where they are available, and when they may become available.

- To manage and monitor the timeline of activities; to reassign tasks, and reprioritize actions dynamically, based on the impact of the incident, Service Level Agreements, and the skills & capabilities of recovery teams.
- To monitor Recovery Time Objectives to assure that the needs of the organization are met – and make strategic adjustments to ensure that the most critical needs are met first, even if at the expense of less critical requirements.
- To track and manage resources, and assign people, space and equipment where needed; to put those assets to their best and highest use, according to the needs of the moment – and the projected needs of activities to follow.

Communication

From the early days of Disaster Recovery Planning, Call Trees have been a mainstay of BCM. With today's auto-notification capabilities, the classic Call Tree may soon go the way of the horse and buggy. Call Trees focus on communication according to organizational structure. But Incident Ready communication requires much more flexibility.

Certainly, the ability to notify all employees of a disruption is essential. But the ability the IMT must think of employees as assets, and must have the ability to identify key assets (those with specific roles, skills or other attributes), and reach out to them on an ad hoc basis. The IMT may need to poll

groups or Teams to determine their availability, in much the same way as they assess the availability of work space or physical assets. Providing that capability depends on more than just a phone bank in the EOC; it requires that Teams (organized by responsibility, skill, location or other attributes) be created as part of the planning process. It also requires that contact information (whether by auto-notification, phone or email) be up-to-date at all times. Updating contact information in the Call Tree once a year won't help you be Incident Ready.

While 'public' communication must be carefully managed (preferably by communication professionals who work with the IMT to shape the messages delivered), the vital communication roles of the IMT also includes effective internal communication – both inbound and outbound. Executives and business managers must be kept informed of the status of progress, in as close to real-time as possible.

Senior managers will need 'dashboards' to monitor their areas of responsibility. Absent the ability to easily access status information, management will try to 'pull' that information from their recovery team leaders – diminishing the time such leaders can devote to the actual tasks at hand. The means to gather status information and the capability to provide senior management easy access must be planned in advance.

Recovery teams must be able to receive updated instructions. And those same recovery teams must be able to 'push' status information to the IMT to enable it to do its job effectively. Preplanning the capacity to communicate collaboratively is critical to the success of the IMT, and a critical component of Incident Ready planning. Whether that collaboration includes text messaging, on-line chat and white boarding, auto-notification, pre-determined conference lines or any other means, they must be planned (and publicized) in advance to be truly useful

Monitoring Plan Execution

To enable the IMT to monitor the status of recovery plans, those plans must be created in 'actionable' form. They too must be Incident Ready.

- Plans must be composed of actions, tasks and activities whose time to complete can be measured. When a task is completed, the IMT needs to know it.
- Plan tasks must take into consideration the dependency of other recovery activities upon their completion. If some other recovery team is waiting for the completion of another team's task, that must be clearly understood.
- To be Incident Ready, plans should focus on dependent assets (people, technology, process, facilities and supply chain) rather than scenarios. Because a plan focuses on assets, a recovery team can create an ad hoc recovery strategy based on the impact of the disruption on their specific assets. An asset-based plan becomes an 'all hazards' plan – able to be executed under any circumstances (rather than a scenario-based plan, for which the assumptions in the scenario must be true for the plan to be useful).
- Plans should contain all of the information and materials – instructions, checklists, critical documents, contacts, etc. – necessary to recovery. Time is the enemy of Incident Readiness; waiting for a file box to be retrieved from off-site storage, or for a shared drive to be restored runs counter to timely, effective recovery.

Actionable plans allow recovery leaders to report measurable progress, to identify issues, roadblocks and resource needs. The IMT, in its Control role, can respond to those facts. It can push progress information out to those who need it; it can escalate issues, dismantle roadblocks and reallocate resources to meet the critical needs of recovery teams.

Real-time event tracking

When the adrenaline is flowing and the IMT and recovery teams are focused on making progress, tracking events is often an after thought (if a thought at all). But tracking activities as they occur is essential for several reasons

- Incident response may be subject to internal audit
- Incident activities may have a bearing on insurance or other legal claims
- The successes and failures of today's incident response can be used to improve plans to make them more viable in the next disruption.

Attempting to recap activities after-the-fact is an exercise in futility. To be thorough, truthful and useful, recovery activities must be tracked as they happen – not as someone remembers them happening.

Are You Incident Ready?

- Are the critical resources and vital interdependencies within your organization known?
- Is your EOC just a room, or a tested, well-equipped command center?
- Does your Crisis Management or Incident Management Plan address Command, Control and Communication requirements? Has it been tested?
- Is the role of your IMT well understood? And has the Team been tested?
- Are all of your Recovery Plans actionable? Have they been tested with the participation of the IMT?

Just having plans and an EOC is not insurance that your organization will be able to weather a disruption. But careful planning, and vigorous testing, can assure that your organization will be Incident READY.