DITY™ Weekly Newsletter
itSM Solutions®
IT Experience. Practical Solutions
The workable, practical guide to Do IT Yourself
Vol. 5.37 • September 17, 2009

Continuity Management – Planning for Unnatural Disasters

By Rick Lemieux

Many IT professionals have followed the path of planning for natural disasters like power outages due to tornados etc. But how many have planned for unnatural disasters like identify theft and software viruses?

Natural disasters like floods and fires can cost enterprises significant lost revenue and customers. Unnatural disasters like identity theft and software viruses can be even more costly. IT organizations need to consider both natural and unnatural disasters when using ITSM best practices to prepare their disaster responses.

As a practitioner in the business of IT Service Management, I have seen many business executives take chances with their approach to Business Continuity Management (BCM). While business issues like supply chain management are outside the scope of most IT departments, IT Service Continuity Management (ITSCM) is not.

ITSCM is a sub-set of BCM focused on establishing the risk-appetite of the business, and then providing recommended planning guidance to the business and IT processes. The ITIL describes the goal of IT Service Continuity Management (ITSCM) as "...to support the overall Business Continuity Management process by ensuring that the required IT technical and services facilities (including computer systems, networks, applications, telecommunications, technical support and Service Desk) can be recovered within required, and agreed, business timescales."

Based on my experience, this newsletter outlines six steps I believe IT organizations should follow in order to build an effective ITSCM program to protect IT services and systems from those unnatural disasters that could have a devastating impact on the business.

IT Service Continuity Management

Step #1 - Managing the Big Picture
IT organizations, through the use of ITSM best practices, need to provide executive management with a holistic understanding of what IT does for the business, how it does it and the impact it will have on the business if it does not continue to do so. In many cases, this will be the first time the management team sees a complete view of IT's contribution to the operational business which will help them make better investment decisions in the area of IT business continuity management.

Step #2 - Scenario planning
IT organizations need to help executive management understand the details of what it would take to recover from an unnatural disaster. Scenarios should include detailed timelines and information about the people, process and technologies required to restore the services to business level operations.

Step #3 – Consultants & Training
If you need to hire a consultant, it is very important to hire individuals or organizations who not only focus on extracting information and delivering reports but those that deliver their final product as a series of training /mentoring sessions that engage the internal (or external) Continuity Management team. Ideally, the consultant will act as a mentor to the team and enable them to acquire the knowledge and skills to maintain and update the program long after the consultants disappear.

Step #4 - In-source or Outsource
Executive management need to understand their continuity options – in-source or outsource. IT organizations need a model that helps identify what continuity services should be sourced internally and what should sourced externally. The

internally sourced services are prime candidates for investment, as they are critical to the success of the business. The business may out-source other activities according to the capability of the enterprise using established sourcing policies and guidelines.

Step #5 - Software

Business continuity management is all about executing a recovery process that involves people, process and technologies. Automating some or all of the recovery process has the potential to help the enterprise get to the business operations state faster. The challenge is to find vendors that actually have off-the-shelf software solutions vs. those that offer custom-built solutions that are cost-prohibitive to the enterprise.

Step #6 Documentation

We have seen too many examples of corporate recovery procedures that require you to read six chapters of project history, steering committee minutes, etc. before you get to the first recovery step. History and reason are important, but only when planning the business continuity management program. The final set of documents needs to be streamlined to enable the Continuity Management team to implement the processes that will get the enterprise to the business operations state as quickly as possible.

Summary

Unnatural disasters in IT are becoming more commonplace than hurricanes, fires, floods, and ice storms we usually associate with disasters. One can also argue that unnatural disasters are even more devastating than their natural counterparts are.

Enterprises need to think beyond the four walls of the buildings they occupy when building their IT Service Continuity program. The six steps to effective IT Service Continuity Management are:

1. Managing the big picture
2. Scenario planning
3. Consultants & training
4. In-source or outsource
5. Software
6. Documentation