

Convergence of Enterprise Protection and Risk Management Methods

By: Ralph Petti, MBCI – President, RP Risk Advisors, LLC

Webster defines the act of “**Convergence**” as “the moving toward a union or uniformity in a scenario.” A second definition from the same source proclaims “Convergence” as “the merging of distinct technologies, industries, or devices into a unified whole.”

In business, this term is being newly adopted to ensure that your Risk Management preparation is truly coordinated, understood and practiced by all parties. A key factor in a successful enterprise recovery planning effort is the communication between all of a firm’s business departments and all locations.

At the time of a disaster event, the ability of every organization to work together in order to achieve a successful recovery for the entire business is essential. The concept of “Convergence” was highlighted in an article in the August, 2005 issue of Security Management magazine entitled “Convergence between Security & Business Continuity.” This article served as a beacon for all to denote that if one organization or process were to break down, the whole process could suffer.

There are many terms that some view to be interchangeable in this industry – Disaster Recovery, Business Continuity, Crisis Management, Emergency Management, Risk Management. Add to that Physical Security, Network Security, Telecommunications Security, Biometric Security and others and you have the makings of a truly enterprise view – truly cyclical and interdependent upon one another.

In today’s enterprise environment, are there more gate-keepers than there are gates sometimes? How do you keep them all on the same page? How do you keep only ONE list to grant specific access? How do you prioritize everyone’s interest in being the number one, most critical area of the business?

All of these questions must be answered. To make sure that everyone is prepared in a contingency scenario, one has to gain management support to require that personnel in all organizations are on the same page. The trend for management to provide such support is certainly on an upswing knowing that there is much more at risk than the loss of data or the loss of production. The terms “integrity”, “security” and “survival” suddenly have new meaning.

So, where do we begin? Granted, all companies are doing **something** for their Enterprise Protection and Recovery Methodologies. Is it enough? Does the inception of a traditional Business Impact Analysis or Risk Assessment mean that everything is fine and there will be no risk at time of disaster? Perhaps you need to look at the fine threads between all processes – the overlaps, the dependencies.

However, does the BIA include a link to other key business organizations such as Security and Telecom? Has there been one list of tasks established for everyone to follow? Has there been a true evaluation and a priority established in consideration of all business units and all requirements? Does everyone know what to do? Will everyone follow their own recovery plans in a live disaster situation?

During any disaster scenario, the companies that recover most expeditiously and experience the least amount of loss of resource are those that are prepared across the enterprise. That has to be the focus. If your organization has not taken a 100% view of your recoverability you may fail to recover.