



Real-Time Business Continuity Strategic Planning

Jeff Allen and Richard Rohrer
Atlantic Communication Services

For years, companies have sought to leverage economies and greater standardization through establishing bulk-purchase arrangements with selected vendors and implementing comprehensive integrated processes and systems for coordinated product and service production and delivery.

Today, however, the implication of these multi-vendor relationships reflect potential jeopardy that corporations must now address, given the risk to company viability, as well as the liabilities associated with not taking action should disaster threaten. It is imperative that all companies evaluate potential threats, prepare contingency plans and establish backup and repair readiness plans, prioritized based on single points of failure and key dependencies so business operations are minimally impacted.

By establishing a cross-organizational plan for threat management, companies can preclude the potential liabilities from not have establishing procedures across communications, personnel, operations, distribution, and financial business areas. Recent business impacts substantiate the criticality of preparedness planning:

- 80% of businesses without business continuity preparedness close within 2 years of a major disaster¹
- 50% of firms that do not recover operations within 10 days of a disaster never recover²

It is imperative that critical business functions be reestablished within 5 days, giving new impetus to conducting threat analysis to model vulnerabilities and results. Comprehensive planning should include scenario assessment, including:

Natural Threats	Intentional Threats from Outside
Unintentional Threats	Intentional Threats from Within

These types of analyses typically begin with a high-level overview of the firm, the mission and objectives, the geographic landscape, and the method of doing business (e.g. use of agents/channel partners/value-added resellers, types of customers, shipping procedures); followed by a determination of all executive processes and operations. Following documentation of the high-level business model, key processes, organization interactions, and information exchange requirements across the enterprise must be documented, with subsequent drill-down of each focused business area, such as an inventory of key assets, programs, and operations/distribution systems, with associated detailed documentation.

At this point, initiation of detailed disaster threat scenario analysis can begin, including quantifying the financial impact of these threats, for both their cost of mitigation and the penalty of risk exposure. These impacts will be analyzed and rationalized across all key business areas, so plans can be put in place, including executive succession, improved insurance coverage, downstream vendor vulnerability hardening, personnel policy and procedures, and communications documentation. Using a structured analytical approach ensures development of a strong plan consistent with corporate strategic objectives while incorporating appropriate vendor performance requirements, HR and contract management policies, financial records

¹ Source: K. Sibley, "Data Recovery: How Safe is Your Business", Computing Canada, Vol. 23, No. 21, Oct 1997.

² Ibid.



**Real-Time
Business Continuity**

management, IP security, copyright and patent rights protection and insurance coverage policies, document management procedures, software applications/license policies, facilities surveillance, operations management and more.

Real-Time Business Continuity (RTBC) is predicated on structured analysis and quantification of potential risk, with prioritized recommendations for remediation address and approaches for mitigation. Ideally, RTBC is best pre-planned methodically, so that policies, procedures, and controls can appropriately be detailed, communicated, and practiced far before they are required under duress, so corporate risk management is optimally managed.