

Business Continuity Planning – What does that mean?

by Manuel Navarro, *Praxis Computing, Inc.*

Business Continuity Planning is a term popularized over the last two decades and has evolved from planning in the event that there is an earthquake to planning in the event that there is an earth-shattering e-virus. How is the evolution of threats facing business today relevant to your business? How much downtime can you afford on your network? Moreover, how should we be thinking about planning for these threats to our business systems and critical data, and what steps should we be taking to protect ourselves? As my father once told me, *“Preparation and planning prevent poor performance.”* (I took the liberty of editing the explicative.)

What is Business Continuity Planning? Business continuity planning is the process whereby businesses ensure the maintenance or recovery of operations, including services to customers, when confronted with adverse events such as natural disasters, technological failures, human error, malicious code, viruses and/or cyber terrorism. The objectives of a business continuity plan (BCP) are to minimize financial loss to the company; continue to serve customers and mitigate the negative effects disruptions can have on a business' strategic plans, reputation, operations, market position, and ability to remain in compliance with applicable laws and regulations. In order to ensure that your business remains healthy through difficult and unforeseen interruption, it is of paramount importance to have robust business continuance plan BCP.

Companies increasingly depend on computer-supported information processing and telecommunications. The increasing dependency on computers and telecommunications for operational support poses the risk that a lengthy loss of these capabilities could seriously affect the overall performance of the company. Information technology and automated

information systems are vital elements in most business processes. IT systems are vulnerable to a variety of disruptions, ranging from mild (e.g., short-term power outage, disk drive failure) to severe (e.g., equipment destruction, fire) from a variety of sources such as natural disasters to terrorists actions, and even cyber-crime.

Because these IT resources are so essential to an organization's success, it is critical that the services provided by network systems are able to operate effectively without excessive interruption.

Downtime impairs productivity: Employees individual production can be drastically affected, when multiplied by the number of hours out, times the burdened hourly rate; it can equal a huge loss for the small business and enterprise alike. Not to mention direct revenue loss, compensatory payments, lost future revenue, billing losses, investment revenue losses leading to impaired financial performance, revenue recognition, affected cash flow, lost discounts, payment guarantees, credit rating, and even your company's stock price.

Other expenses may include temporary employees, equipment rental, overtime costs, and related travel expenses. A survey by the FBI and Computer Security Institute (www.gocsi.com) found that in 2001 the financial loss due to network disruptions among 186 surveyed companies was nearly \$378 million, compared to \$266 million reported by 249 respondents in 2000. The average cost was, therefore, approximately \$2.0m in 2001, up from \$1.0m in 2000. But this is only a fraction of the true cost.

Albert Einstein once said, *“Intellectuals solve problems, geniuses prevent them.”*

Here are some steps to keeping your network available and maintaining your company's business continuity.

- o To effectively determine the specific risks to an IT system during service interruption, a risk assessment of the IT system environment is required. A thorough risk assessment should identify the system vulnerabilities, threat, and current controls and attempt to determine the risk based on the likelihood and threat impact. Because risks can vary over time and new risks may replace old ones as a system evolves, the risk management process must be ongoing and dynamic.
- o Conduct a Business Continuity Planning (BCP) Workshop: A BCP Workshop helps to identify and prioritize critical IT systems and components. Executive Management should be involved to help identify preventive controls and review measures taken to reduce the effects of system disruptions that can increase system availability and reduce contingency life cycle costs.
- o Consider a BCP assessment which can identify critical systems whose loss could cause a major impact to the company. This assessment process should be repeated on a regular basis to maintain the health of the organization. Assessments identify threats and vulnerabilities so that appropriate controls can be put into place to either prevent incidents from happening or to limit the effects of an incident.
- o Build strong architecture, consider redundant communications paths, lack of single points of failure, enhanced fault tolerance of network components and interfaces, power management systems with appropriately sized backup power sources, load balancing, and data mirroring and replication to ensure a uniformly robust system.