Crossing the Digital Divide (v85)

"It's not rocket science"

by Joseph Feigon

for the Observer

As many of our friends, family and neighbors begin to rebuild their lives following the devastating fires earlier this month, it's time to remind our county leadership we're not getting what we've been promised, and the only reason change hasn't occurred is greed. A single strand of fiber-optic cable running up the 101 corridor has been severed, burned, vandalized and abused, and yet, despite increasing pressure from the stakeholders, much of Sonoma, Mendocino and Humboldt Counties remain exposed to failure prone infrastructure with no apparent plans to address this increasingly dangerous and irresponsible lack of service.

This week's column is about basic survivability, a primer for any Network Engineer, Corporate Information Officer, or local business.

Business continuity encompasses planning and preparation to ensure that an organization can continue to operate in case of serious incidents or disasters and is able to recover to an operational state within a reasonably short period. As such, business continuity includes three key elements and they are

1. **Resilience:** critical business functions and the supporting infrastructure must be designed in such a way that they are materially unaffected by relevant disruptions, for example through the use of redundancy and spare capacity;
2. **Recovery:** arrangements have to be made to recover or restore critical and less critical business functions that fail for some reason.
3. **Contingency:** the organization establishes a generalized capability and readiness to cope effectively with whatever major incidents and disasters occur, including those that were not, and perhaps could not have been, foreseen. Contingency preparations constitute a last-resort response if resilience and recovery arrangements should prove inadequate in practice.

Typical disasters that business continuity is meant to account for include natural disasters such as fires and floods, accidents by key personnel in the business, server crashes or virus infections, insolvency of key suppliers, negative media campaigns and market upheavals such as stock market crashes. Such disasters may not necessarily have to occur in the place of business to have catastrophic impact in the globalized economy.

The management of business continuity falls largely within the sphere of quality management and risk management, with some cross-over into related fields such as governance, information security and compliance. Risk management is an important tool for business continuity as it provides a structured way to identify the sources of business disruption and assess their probability and harm. It is expected that all business functions, operations, supplies, systems, relationships, etc. that are critically important to achieve the organization's operational objectives are analyzed and included in the business continuity plan. Business Impact Analysis is the generally accepted risk management term for the process of determining the relative importance or criticality of those elements, and in

turn drives the priorities, planning, preparations and other business continuity management activities.

One important way to achieve business continuity is the use of international standards, program development, and supporting policies. These standards ensure that proven methods and concepts for business continuity are used. As with many quality management standards though, the primary task of identifying relevant potential disasters, making plans for evacuation, buying spare machines and servers, performing backups and bringing them off-site, assigning responsibility, performing drills, educating employees and being vigilant cannot be replaced by adherence to standards. As such, commitment by management to see business continuity as an important topic and assign people to work on it, remains the most important step in establishing business continuity.

If there is no Business Continuity plan implemented and the organization in question is facing a rather severe threat or disruption that may lead to bankruptcy, the implementation and outcome, if not too late, may strengthen the organization's survival and its continuity of business activities (Stuart Gittleman, 2013).

Content source summarized on Wikipedia.

Control those things you can, and keep the surprises to a minimum!