Disaster Strikes: Will Your Business Survive?

Source: The Business Owner (http://www.thebusinessowner.com)

Business owners invest, strategize and labor year after year to grow revenue, market share, profit and capabilities. Much or all could be instantly lost if a disaster strikes. With proper disaster recovery planning (DRP), losses can be limited to acceptable levels. But few businesses have a disaster recovery plan. Most small and mid-size businesses remain at risk.

The risks of not having an effective recovery plan can go beyond the loss of assets physically destroyed in the disaster. Legal action can be taken against a business, its owners and executives if they are negligent in their duty to take reasonable precautions to protect others from harm. Damaged parties and potential claimants can include customers, shareholders, creditors and lenders.

Faced with the risk, why do business owners fail to plan? First, disasters are random and rare, so the tendency is to assume that it won't happen to you. Second, the payoff is uncertain for efforts taken to avoid such a loss. Owners naturally want to dedicate their limited capital (time, money and labor) towards more predictable returns. Neither reason is acceptable given what is at stake.

If you are a business owner, ask yourself this question, "How would my business be impacted if my physical facilities disappeared tonight?" In effect, this could happen with a fire, flood, earthquake or explosion. If the answer is unacceptable, then you need a disaster prevention and recovery plan. The cost in time and dollars to develop and implement one do not need to be significant. Use the following as a guideline.

Step One: Identify What You Cannot Live Without

The first step is to identify your most critical assets. Do so by listing the assets that you and your business use in the creation and delivery of your goods or services and in the operation of your business. The primary asset categories are facilities, personnel, data, network/connectivity, voice, hardware and software. Add to the list items that are necessary to prove ownership of valuable assets, rights or interests such as titles and insurance policies. Then rank each asset or asset class from most valuable and/or critical to least valuable and/or critical. Estimate the impact that each asset would have if lost. Quantify the impact in dollars, customer relationships, public perception and contingent liability.

Step Two: Reduce the Likelihood That Disaster Strikes

The second step is to reduce or eliminate the likelihood that a disaster occurs. Begin by listing any perils that could cause damage or loss to one or more of the assets that you listed for step one above. Disasters, referred to as perils in the insurance industry, include: fire, flood, tornado, earthquake, bombing, riot, etc. Initiatives could include updating electrical wiring, installing and maintaining fire extinguishers, moving computer data and systems from a basement where flooding could occur, or locating in an area protected from tornados. Implement strategies that offer the highest reward as it relates to the associated cost.

Step Three: Develop a Survival Plan

Step three is to develop a plan for minimizing loss if a disaster strikes. To do so, consider each asset listed in step one and develop ways to mitigate or recover from loss. This might include backing up critical data computer data, storing data off-site, buying and maintaining an electrical generator, and developing a detailed action and recovery plan. Consider the maximum length of time that you can tolerate being without the use of each asset or capability. The recovery plan should adhere to these thresholds.

Next, identify disaster recovery teams, team leaders and their alternates. Consider having leaders carry disaster recovery cards in their wallets or purses at all times. Include important phone numbers, addresses, meeting places and action steps. Assess the merits of having pre-written scripts that can be issued to the media upon the occurrence of a disaster. Include in your plan the location of your temporary or alternative office or how the location will be determined.

Step Four: Test the Plan Periodically

The final step is to test, implement and periodically audit the plan. Test to make sure the plan, and each component of the plan, works. Check every step before you adopt it. Don't bet your company on a plan you can't test. When the bugs are worked out, implement that plan and make all employees aware of it and their responsibilities. Periodically check to be sure that the plan is being maintained. For example, make sure back ups are being made of data, and that the backups are of acceptable frequency and quality.

A terrific resource for additional information, products and services is the 'Disaster Recovery Yellow Pages,' that can be found at www.disaster-help.com or by searching the Internet by the same name. There is also software that can help. Business Impact Analysis Software helps a company assess the impact that a disaster could have. Recovery Plan Development Software assists in the development of a recover plan.

In summary, don't gamble your life work or your career on whether or not a disaster will hit your business. Assess the risk, develop a plan, make sure it works and then test it regularly. Do so and you will sleep better and your business will be more likely to survive for the long run.