Katrina tested our Contingency Planning and taught us Contingency Management!

Hurricane Katrina brought out the best and worst in all of us. Our best was highlighted by an international outpouring of recovery resources. Our worst was highlighted by the few who chose to focus on the looting, the shooting, and the failed rescue efforts. Most of the finger pointing was driven by fear and frustration. Unfortunately some was exaggerate by those creating sound-bites for the next election.

Fact is, the hurricanes of '05 taught us much of what we already knew. They taught us that bad things happen to good people when they don't heed the warnings of imminent danger. They taught us that failing to plan is planning to fail, and no matter how much we plan, we need a system of command and control to lead us out of harms way.

Contingency Planning – Conclusions and Recommendations:

Risk Management (RM) assessments during Katrina underscored the importance of well written and tested contingency plans. For the most part plans required by financial institution regulators, those written for the private business community and those recommended for schools, elderly and child care facilities, and hospitals worked well. It appears the plans written for insurance companies and financial institutions scored the highest followed by those written for schools and public utilities. Most other plans failed because they were outdated or written to the "Disaster Recovery" standards of the '70s the "Business Continuity" standards of the '80s and '90s, or the "Business Resumption" standards acceptable prior to 9-11. Contingency plans written and updated to post 9-11 protocols worked best until they too were overwhelmed by incident "scope creep," and the escalating breakdown in communications followed by a failure to command and control the response from the private sector.

RMLC Solutions:

Contingency plans in the future must include "contingency management" so all potential responders are familiar with and know their role in the "Unified" Incident Command System. Corporate security and building maintenance personnel should be trained and ready to conduct initial damage assessments, estimate the immediate and potential scope of the incident, and know how to launch an appropriate response and recovery strategy.

RMLC Solutions:

Insurance companies call it "Indemnification," business leaders call it "Business Resumption," community leaders call it "Survival." We call it "getting back to normal." Our ultimate goal when disasters strike is to get victims back to a like and similar position they were in prior to their loss. Risk Management workshops in 2006 will adopt the Incident Command System (ICS) to every walk of life, using the National Incident Management System (NIMS) as our performance standard.

The Risk Management Learning Center

Natural Disasters -- Contingency Planning for Contingency Management

Written by

Rich Woldt CEO: The Risk Management Learning Center

Please share this brochure with your Board of Directors, Management Team, Contingency Planners, Contingency Managers, Personnel and Security Managers, Employees and Community Leaders!

This flyer can be downloaded free from the RMLC web site @ rmlearningcenrter.

RMLearningCenter.com
Rich@RichWoldt.com

Customize Your Contingency Plans: Too often contingency plans are outdated because employees, buildings, and operations have changed and no one remembered to adjust the contingency plans. Customize recommendation in this brochure to fit your special needs and personal situation. Create a written action plan and incorporate it into your business contingency plans. Develop your own family emergency evacuation plan from your home and place of employment. Annually, review building evacuation plans designated by you employer, local fire department, and Director of Emergency Government. Discuss your own "best" evacuation route from your home to a relative or friends in another state. Write your own family contingency plan and share it with your neighbors.

1. **Benchmark Your Company's Contingency Plans:** Obtain a copy of the "Paid Paranoid" by Paul Bergee and conduct your own evaluation of your business' or employer' contingency plans.

Fraud, Embezzlement, Scams & White Collar Crimes:

Embezzlers, scam artists, and normally honest people are all motivated by economic need. Take away someone's means of support and by definition there will be an incentive to perpetrate a scam, fraud, and embezzlement to meet their needs. Justifications will include, "Everyone is doing it, I have no choice, they owe it to me, and I'll pay it back someday." Embezzlers who have already begun to embezzle will make one last effort and use the disaster to cover their tracks. The following recommendations will strengthen you defense against the seasoned embezzler while discouraging an honest person from doing something illegal during a time of desperation.

1. **Take Control of Building Access:** Businesses should make sure no one person has all the keys, combinations, passwords, etc. to make it from the parking lot to the cash items stored on premise. Separating access controls so it requires more than one person will discourage burglary, robbery, extortion, and efforts to conceal a fraud or embezzlement.
2. **Take Control of Administrative Access Codes:** Computer, website, wire transfer, and internet banking systems are all designed and maintained by an administrator. Computer fraud such as the creation of fictitious accounts, website fraud such as phishing and pharming, wire transfer fraud such as money laundering, and internet banking fraud such as unauthorized closing of accounts, is common before during and after disasters. Therefore, business owners and internal auditors should closely monitor all administrative transaction immediately before, during, and after a disaster. Immediately following the disaster, all administrative access codes should be changed.
3. Losses from white collar crimes can easily exceed personal property losses during a disaster. Therefore, administrators, while they might need access to maintain your systems should not have total control over your computer, website, wire transfer, or internet banking systems.

    - Access codes should be authorized and distributed on a "need to know" basis and changed frequently to discourage an ongoing embezzlement. Administrative duties should be rotated on a surprise basis and system file maintenance reports should be reviewed quarterly to ensure all system changes and maintenance performed was authorized.

We all learn from our mistakes. So while the pessimists focus on blaming others for what went wrong during Katrina, I encourage you to take the optimistic high road and focus on process improvements that will better prepare your family, your employer, and your community for the next life threatening challenge.

You can access the RM research links and white papers used to prepare this brochure at… The Risk Management Learning Center's web site rmlearningcenter.com

Rich Woldt CEO
The RM Learning Center