

Business Survival Newsletter™

go to www.rothstein.com

BUSINESS SURVIVAL™:
A BUSINESS CONTINUITY NEWSLETTER FOR DECISION MAKERS
FROM ROTHSTEIN ASSOCIATES INC.

Volume 7, Issue 2: Copyright 2004, Rothstein Associates Inc.

FEATURE ARTICLE:

SEVEN ITEMS OFTEN OVERLOOKED IN DISASTER PLANNING

by Steven Lewis, Ph.D.

During the last 20 years, we have worked with organizations ranging from Retailers to Universities, from Banks to Dairies, from insurance companies to local governments and beyond. In all of these situations, we have found that all planners, no matter how experienced and systematic they may be, tend to overlook certain items. Some of these are small, but crucial items which simply add insult to injury when disaster occurs, but other can threaten the survival of the organization.

These seven overlooked items fall into a number of general areas, which are listed below and then discussed:

- 1 Missing things “too close to see”**
- 2 Ignoring employee’s relevant personal-life situations**
- 3 Failure to track out-of-the-ordinary situations**
- 4 Intuitively assuming how other departments function**
- 5 Not learning needs of emergency organizations outside of the company**
- 6 Forgetting "unforgettable" events**
- 7 Ignoring external factors**

1. MISSING THINGS “TOO CLOSE TO SEE”

An example of this oversight, which we have seen in almost 100% of the facilities we have examined, is the vulnerability of network and telephone panels to falling water. Most facilities have a panel on a wall where the telephone wires enter the building. Typically this is not covered and in the event of water coming down the wall, they burn out and are destroyed. Similarly, most computer networking racks are exposed to reduce heat buildup, however, they are not shielded from nearby sprinkler heads or simply water coming from above the ceiling and following the cables down to the rack. When they are hit by water, they also burn out.

Another overlooked item we have frequently seen, particularly in older buildings, is the need for a key to exit a building via a locked door. Often institutions which are open to the public, such as banks, lock their doors but remain open for many hours after their public hours have ended. Every exit door needs to be operable from the inside without a key.

Another frequent condition is the use of non-fireproof safes to protect key documents. Most safes are burglar-proof; however, most are not insulated, and in a fire, the contents are incinerated.

Also overlooked are the two most important documents in any disaster: company checks and purchase orders. A supply of these needs to be kept off-site, ready to purchase immediately-needed equipment and supplies.

Additionally, many organizations have valuable paintings, displays, and antiques in their facilities. Often these are not covered by insurance riders in the event they are destroyed.

2. IGNORING EMPLOYEE'S RELEVANT PERSONAL-LIFE SITUATIONS

Often, an organization's disaster plan requires key employees to relocate to a computer hot site for the duration of an emergency. We have found in several situations that those employees were single parents or care-givers, with no ability to even work emergency overtime, much less relocate out of the region to a hot site. One technique we have used to uncover such situations is to have all employees sign a form indicating that they have read and understood the disaster plan, as it pertains to them, and that they can fulfill their assignments in carrying it out.

3. FAILURE TO TRACK OUT-OF-THE-ORDINARY SITUATIONS

Many disaster plans become fixated only on the disaster itself, rather than trying to track abnormal situations which can make the disaster worse. One of the most frequent out-of-the-ordinary situations to occur is that of temporarily disabled employees - requiring special assistance to exit the facilities. Planners need to have a system in place whereby these employees are identified and someone is tasked with ensuring their safety.

Another situation occurs when key employees go on maternity, military or other extended absence with the result that their functions are left without emergency backups. Planning for their absences needs to also include the emergency backup they provided.

Labor unrest represents a major vulnerability for many organizations. Planners need to set up a responsibility for tracking the expiration dates of union contracts to properly assess the company's evolving risk exposure in this area.

4. INTUITIVELY ASSUMING HOW OTHER DEPARTMENTS FUNCTION

All organizations depend on a series of support functions. The most typical of these are: mail delivery, check printing, voicemail, janitorial, and personnel. Because of their familiarity, planners often don't spend the time going through the details of their operations. The oversights we have found include:

- an accounting department with a customized check-printer, using blank check stock – requiring over a week to replace the printer;
- a mail room having no records off-site to enable notification of couriers and delivery services such as Fedex where to deliver when the facility is not in operation;
- lack of an ability to access employees' voicemail if they are incapacitated;
- personnel files stored in the executive department, in polished mahogany file cabinets,
- lack of a procedure to track locations and proper protection of hazardous materials used by janitors and exterminators, which could, in a flood or fire, be spread throughout the facility.

Beyond these, many organization have “after-hours” facilities, such as banks having night depositories for large commercial customers. Often we have found that there is no way to notify these important customers if the facility becomes unavailable.

5. NOT LEARNING NEEDS OF EMERGENCY ORGANIZATIONS OUTSIDE OF THE COMPANY

Particularly in this age of consolidation, many organizations have far-flung locations. We have often found that the local fire and police departments covering these locations do not have up-to-date contact information in the event of an emergency in the local facility. For more complex facilities, we have almost never found that a set of building plans has been filed with the local fire department.

6. FORGETTING “UNFORGETTABLE” EVENTS

Almost all organizations we have worked with have had major disasters which have entered into their corporate lore. However, typically they fail to document the details of what went wrong; what went right; what they've learned; what they need to change for the future; and, a tracking of follow-up on the recommended changes.

7.IGNORING "EXTERNAL" FACTORS

Many organizations don't take proper cognizance of the fact that they are located nearby to areas which can be a focus of demonstrations or targets of violence. An example we encountered after September 11, 2001, was an organization with an office and backup storage site located on an Air Force Base, hundreds of miles away from the terrorist attacks. As a result of the attacks, the base was closed to non-military personnel and the organization was unable to operate or gain access to the facility for an extended period of time.

CONCLUSION

In conclusion, the best way to avoid overlooking items in the disaster plan is by not going it alone. Planners need to seek both internal and external reviews of their plans by experienced personnel who were not involved in the plan development. These reviews can include having people critique the plans of the departments upon whom they are dependent. They can also include having lower-level personnel review plans developed by their superiors. Finally, from the outside, often the organization's insurance company or independent outside audit firm will provide an outside audit of the plan. The bottom line is, there's no substitute for a second set of eyes.

Steven Lewis, Ph.D. is the Editor-in-Chief of the Disaster Recovery Yellow Pagestm (www.DisasterRecoveryYP.com). He is a Certified Information Systems Auditor (CISA) with a PhD in Systems from the Univ. of Pennsylvania, and a Masters and Bachelors in Engineering from Cornell University.

During the last fifteen years, he has developed over 120 comprehensive disaster recovery/business continuity plans for networked based organizations. All of these plans were subject to review by Regulatory Agencies and were all approved. Many of these also included "Year/2000" risk analyses, evaluation and testing.

Dr. Lewis has also authored numerous articles, including "Plan for a Disaster Without Destroying Your Budget," which appeared in PUBLIC RISK magazine, and "Disaster Recovery Planning A HIPAA Requirement," which appeared in HEALTH FACILITIES MANAGEMENT magazine.

=====

SPECIAL OFFER!
DISASTER RECOVERY YELLOW PAGES
COMBO - PRINT PLUS CD-ROM EDITIONS
Save \$20.00!

The only comprehensive sourcebook designed to help users locate scores of crucial but hard-to-find recovery services throughout the United States and Canada. It contains over 3000 vendor listings and covers over 270 categories. The CD now contains active links to web sites.

2004, CD-ROM + 350 Pages. Order #DR673.
<http://www.rothstein.com/data/dr673.htm>

VENDORS:

OBTAIN A FREE LISTING IN THE NEW 2005 EDITION OF THE DISASTER RECOVERY YELLOW PAGES

The 2005 edition of the Disaster Recovery Yellow Pages is in final preparation and vendors who have not sent their request for a free listing are invited to do so now by visiting www.disasterrecoveryyp.com to mit their listing information.

Based on nearly two decades of disaster planning experience, the Disaster Recovery Yellow Pages is a 350-page comprehensive sourcebook designed to help users locate scores of crucial but hard-to-find recovery services throughout the United States and Canada. The Disaster Recovery Yellow Pages contains over 3000 vendor listings and covers over 290 categories such as drying & dehumidification of paper & microfilm records, smoke odor counteracting services, trauma counselors, salvage, emergency rental of network and other computer equipment, etc.

The sourcebook is used by facility managers, computer operations managers, emergency personnel, risk managers, security managers, librarians, record managers, systems executives, and business recovery coordinators, as well as claims adjusters, insurance agents, and others responsible for putting organizations "back to normal" after a crisis. The only comprehensive sourcebook designed to help users locate scores of crucial but hard-to-find recovery services throughout the United States and Canada. It contains over 3000 vendor listings and covers over 270 categories. The CD now contains active links to web sites.

To order: <http://www.rothstein.com/data/dr673.htm>

Vendor Registration:

www.disasterrecoveryyp.com

=====

RECOMMENDED READING

NEW BOOK!

SOFTWARE METRICS: BEST PRACTICES FOR SUCCESSFUL IT MANAGEMENT

by Paul Goodman

Endorsed by the European Software Process Improvement Foundation

(Available: August, 2004; order #DR735).

See <http://www.rothstein.com/slbooks/dr735.htm> for details.

"For over ten years, the sad statistics on IT project failure have barely changed. Survey after survey shows that over half of all IT projects fail (especially large projects) and most projects are delivered over time, over budget. Accurate time and cost forecasting, based on sound performance measurement metrics, could reduce the number of project failures by helping to create more realistic cost / benefit cases. And better software quality would help, too.

"Badly estimated software projects can waste serious money: money that could otherwise be invested in mission achievement, new product development and creating a competitive edge. Poor software quality can lead to poor quality — or even dangerous — products. It can cause public relations and marketing disasters, damage brand reputation and market share. While use

of effective software metrics is not the total answer, it is certainly a crucial part of getting to grips with software development.

“Paul Goodman's book makes a valuable contribution to IT Development Project success. It is comprehensive, lucid and packed with illustrations and practical examples. It is as accessible to the non-specialist as it is to the software guru.”

Andrew Hiles, FBCI, MBCS, Director, Kingswell International

NEW BOOK!

**THE DISASTER RECOVERY HANDBOOK:
A STEP-BY-STEP PLAN TO ENSURE BUSINESS CONTINUITY AND PROTECT
VITAL OPERATIONS, FACILITIES, AND ASSETS**

by Michael Wallace and Lawrence Webber (includes CD-ROM)

“Without careful planning, organizations often do not survive major interruptions in the operation of their business. The Disaster Recovery Handbook gives readers proven processes and techniques to develop a disaster recovery plan and protect their organizations in the face of extraordinary circumstances. Featuring a CD-ROM with templates for process and skill matrices, contact databases, risk-assessment score sheets, and more, the book gives detailed instructions for:

- Assembling a recovery team
- Building an interim plan
- Setting up an emergency operations center
- Recovering vital records
- And more.”
- See <http://www.rothstein.com/data/dr727.htm> for details

SPECIAL OFFER!

**ENTERPRISE RISK ASSESSMENT AND BUSINESS IMPACT ANALYSIS:
BEST PRACTICES**

by Andrew N. Hiles,
plus

**BUSINESS THREAT AND RISK ASSESSMENT CHECKLIST
(WITH CD-ROM)**

by Edmond D. Jones, MBCP

Buy Both Books and Save \$13.00!

See <http://www.rothstein.com/data/dr732prom.htm> for details.

SPECIAL OFFER!

Save \$14.00 on

**BUSINESS CONTINUITY: BEST PRACTICES:
WORLD-CLASS BUSINESS CONTINUITY MANAGEMENT
PLUS**

AUDITING BUSINESS CONTINUITY: GLOBAL BEST PRACTICES

by Rolf von Roessing.

See: <http://www.rothstein.com/data/dr725.htm> for details.

go to www.rothstein.com

=====

Rothstein Associates Inc.
4 Arapaho Rd.
Brookfield, CT 06804-3104
203.740.7400 or 1.888.ROTHSTEIn; fax 203.740.7401
email: pjr@rothstein.com

Newsletter Editor: Philip Jan Rothstein, FBCI ()
Copyright 2003, Rothstein Associates Inc. All Rights Reserved

BUSINESS SURVIVAL™ is sent by YOUR subscription request ONLY!
It is distributed 5 - 8 times each year.
To unsubscribe, email subject "UNSUBSCRIBE."

=====