

# Business Survival Newsletter

go to [www.rothstein.com](http://www.rothstein.com)

BUSINESS SURVIVAL:

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

=====  
Volume 1, Issue 3: Copyright 1998, 2001, Rothstein Associates Inc.  
=====

## IN THIS ISSUE:

Empty-Lap Syndrome?  
Succeeding at Succession Can Avoid Financial Ruin  
Survey Says ...  
Featured Web Site: Contingency Planning & Management  
Industry Headline News  
Recommended Reading  
Y2k Contingency Planning  
Looking Beyond Disaster Stereotypes

=====  

## OUR FAVORITE QUOTE OF THE MONTH:

"Men stumble over the truth from time to time," said Winston Churchill, "but most manage to pick themselves up and run off as if nothing happened."

=====  

## SUCCEEDING AT SUCCESSION CAN AVOID FINANCIAL RUIN

by Andrew N. Karlen, Esq.

Fire, flood, explosions, even widespread theft, can certainly spell disaster for a small company. There is, however, another catastrophe waiting to happen in the form of financial ruin -- the failure to pass the torch of ownership to a new generation of owners and managers.

According to the United States Small Business Administration, nine out of ten businesses in the country are either closely held or family run, but the odds of surviving the transition from the founding generation to the next are slim: only three of ten actually make it. Ownership succession to the third generation is even more unlikely: less than two of ten survive.

To avoid becoming a casualty of these succession statistics, senior management must come to grips with passing on the assets and management control from one generation to the next. How a firm succeeds at succession planning may be the ultimate measure of a company's health and management well-being.

*Continued*

Ownership succession generally falls into one or all of several categories. Most would agree that a best-case succession would be to a family member or members. However, if the conditions are not right for this to take place, succession to the employees of the firm is often another desirable alternative. A third choice could be the sale of the company to outside investors or even competitors. Clearly, the last and worst case would be the forced sale to meet debt or estate tax obligations.

While experts in the field of business continuity planning point to a number of obstacles in the process -- loss of ego, monetary insecurities, uncertainty about the next generation's qualifications most agree that owners in their early 60s should begin addressing matters of management and ownership succession.

However, planning for the transition of management and the transfer of ownership begins with the senior generation grasping the need and becoming secure with the concept. The goal is not for an owner to simply walk into work one day and turn over the reins -- the goal is for the owner to understand that the process is necessary for his or her own lifestyle and retirement needs. This is the only way to ensure that the business, which may have taken a lifetime to build, will survive and flourish for the next generation of family or key employees to enjoy.

Not addressing the future can be a major problem for the founding generation. The earlier the better because it gives owners the most time to select and train their successor(s).

Rethinking what business succession planning really is begins with throwing out the notions that it is a sort of stepchild of estate planning or a mechanism to put the current owner of a business out to pasture. Or, it is believed to be merely the end result of a boilerplate buy-sell agreement. Succession or continuity planning prepares the business and the family for the heavy bite that federal taxes take when a business is passed from one generation to the next.

"Companies should realize that in small, closely-held businesses, a lot of times the value of your estate is bricks and mortar and not liquid assets," said Gerald Mirra of Corporate Plans Associates (Armonk, NY). "In the event of death, when the government comes to collect the estate tax, they want cash, not physical property. Companies that don't plan carefully can be forced to liquidate to pay estate taxes."

"Let me put it another way," Mr. Mirra added. "If I own the World Trade Center, I can leave it to my spouse with no federal estate tax. But when mom dies the government would take one of those Twin Towers away. The estate tax for large estates is essentially 50 percent of what you own. If that isn't a sobering fact for taking action, I don't know what is."

Failure to plan for the passing of the torch can certainly lead to financial ruin. We all know the story of the Miami Dolphin's Joe Robbie and the fire sale of the team and stadium his heirs were forced into in order to meet federal estate taxes obligations.

Indeed, the prospects of a 50 percent tax should be more than sobering, it should be an alarm. Thankfully it is one that sounds before disaster strikes.

---Andrew N. Karlen, Esq., with law offices in White Plains, NY represents businesses in areas of business formation, transactions, planning, real estate and litigation. He is vice chair for Small Business of the Westchester County Chamber of Commerce and Co-Chair of the Corporate and Commercial Law Committee of the Westchester County Bar Association.

*Continued*

--- Succession Planning is just one of the business continuity issues Rothstein Associates' clients face. Contact Philip Jan Rothstein if we may be of assistance.

=====

## Y2K CONTINGENCY PLANNING

According to humorist Dave Barry, "If the Millennium Bug is not fixed, when the year 2000 arrives, our financial records will be inaccurate, our telephone system will be unreliable, our government will be paralyzed and airline flights will be canceled without warning. In other words, things will be pretty much the same as they are now."

According to Steven Davis, Budget Manager, Montgomery County, Maryland Office of Management and Budget:

"I see a real need for both business continuity planning and emergency preparedness for Year 2000 failures for businesses as well as at the local, state, national, and international levels. Currently, little is being done by the public or private sector to develop contingency plans. The federal government has yet to do any preparedness, focusing efforts only on fixing critical systems

Many organizations seem to either be in denial or overly optimistic about the success of remediation efforts. Based on the likelihood of some level of system failures, all organizations should take the following steps:

- a. Develop contingency and business continuity plans for all mission critical systems, looking at the potential for impact including the impacts resulting from the interrelationships of various systems.
- b. Triage to identify systems, institutions, and industries that are most critical and at risk.
- c. Set compliance deadlines (the absolute latest things can be "ready"). In general, systems should be repaired/replaced three months before their individual failure horizon.
- d. Develop a disaster-recovery plan for each system. Disaster-recovery plans for "at risk" systems must be ready three months before failure horizon.
- e. Identify systems that can be repaired as compared to those that are not likely to be mitigated.
- f. Warn citizens and consumers about potential consequences of a computer failure or disruption. Develop recommendations on how to inform people about this potential problem and its effects. Also, identify the impact that such warnings would have on society and the economy.
- g. Develop contingency plans for major service disruptions (power, telecom, transportation)."

Check out <http://www.erols.com/steve451/impact.htm> for Year 2000 contingency planning resources.

=====

## LATE-BREAKING INDUSTRY HEADLINE NEWS!

Sourced from 400+ news providers, so that you can access news stories as they develop, located at [www.rothstein.com](http://www.rothstein.com):

- Disaster Recovery Services
- Weather Events and Natural Disasters

*Continued*

- Risk Management & Insurance
- World Terrorism
- Year 2000
- Information/Data Security
- Internet/Web Security

[www.rothstein.com](http://www.rothstein.com)

=====

### EMPTY-LAP SYNDROME?

According to Safeware Insurance Agency, Inc. of Columbus, Ohio, 799,000 incidents of laptop theft or damage were reported in 1996, up from 591,000 in 1995. What information resides on your laptop, and what would be the impact on your organization if it was lost, destroyed or stolen? Consider:

- Loss of vital information
- Disclosure of sensitive information
- Productivity impact -- how much time would you spend reconstructing work in process?

Drivesavers, Inc., of Novato, California offers these common-sense tips:

- Keep current copies of important data somewhere other than your laptop
- Quit programs before shutting down to avoid data loss and program corruption
- When compressing data, make extra backups because compressed data is more difficult to recover
- Never reformat your drive without testing your backup
- Don't move or jar a drive while it's operating.

=====

### RECOMMENDED READING

(These and other titles are available from The Rothstein Catalog On Disaster Recovery at [www.rothstein.com](http://www.rothstein.com))

#### BUSINESS CONTINUITY PLANNING: STEP-BY-STEP GUIDE WITH PLANNING FORMS

By Kenneth L. Fulmer

This book offers a comprehensive, step-by-step outline filled with precise instructions, risk and business impact analysis guidelines and forms for creating a business continuity blueprint. It serves as a workbook for those organizing a plan, and as a guidebook for those responsible for implementation. Clear and complete, Business Continuity Planning will prove an invaluable resource and guide for managers, owners and planning coordinators.

#### DISASTER RECOVERY TESTING: EXERCISING YOUR CONTINGENCY PLAN

Philip Jan Rothstein, Editor

"... The most widely read source of information on the subject to date... an excellent starting point for both novice and experienced business continuity planners... a feast of ideas that challenge and stimulate." *Survive! Magazine.*

"... focuses much needed attention on disaster recovery testing... written in four well-planned, easy-to-follow sections, with numerous realistic scenarios and ideas to consider... provides useful guidance for management of the entire disaster recovery testing process." Security Management Magazine.

\* \* Price reduced from \$95.00 to \$65.00 + \$6.00 S+H. \* \*

=====

### SURVEY SAYS...

According to 1,320 CIO's and other senior information executives participating in the Ernst & Young LLP / Information Week Fourth Annual Information Security Survey:

% of companies surveyed that experienced information losses due to security failures and disaster in the past two years: 52%

% of losses caused by malicious acts by insiders: 31%

% of losses caused by malicious acts by outsiders: 18%

% of losses caused by natural disasters: 24%

% of losses caused by industrial espionage 7%.

=====

### FEATURED WEB SITE:

#### Contingency Planning & Management (CP&M)

Witter Publishing produces Contingency Planning & Management Magazine, a valuable resource for the business continuity community. Contact Rothstein Associates for subscription information (free to qualified professionals).

[www.ContingencyPlanning.com](http://www.ContingencyPlanning.com)

=====

### LOOKING BEYOND DISASTER STEREOTYPES

Anybody involved in disaster recovery should not find it difficult to recite their own 'top-ten' list of favorite disaster causes. They might include natural disasters such as floods, hurricanes, earthquakes or blizzards; external events such as power or communications failures; technological disruptions like computer crashes or network outages; or, facility events like fires. If one were to conduct a careful analysis of corporate 'disasters' over the past decade, one would find that there are numerous disaster causes or potential causes which are largely overlooked. Recent examples include:

a major financial organization experienced a seven-figure dollar loss because of a single data base corrupted by a programmer who updated a production program without following production signoff and turnover standards or procedures.

a large metropolitan hospital irrevocably lost their entire pharmacy data base including current patient information when a disk crash led to the discovery that the backup tapes they had been

consistently producing nightly for over two years were of the wrong files. No backups had ever been made of the lost data base.

a major research and development facility depending on temporary staffing for their data center operation experienced a two-day disruption when a disgruntled former employee returned unnoticed through the temporary employment agency and sabotaged the data center.

a medium-size service organization experienced severe embarrassment and inconvenience as well as a five-figure dollar loss when their voicemail system crashed and all current messages were irretrievably lost.

a large insurance company experienced a six-figure dollar loss when a utility power disruption forced their data center to rely on backup power. Although their uninterruptible power supply and backup generators were effective for the data center, several hundred employees were put out of work since there was no backup power for business operations in the same building.

a bank was put out of business for over a week and very nearly permanently when a facility disruption necessitated activation of their data center disaster recovery program. Although the data center was operational in less than 48 hours at a recovery site, no business resumption plan had been implemented for the 100+ employees displaced by the same event.

a hundred-employee service organization was nearly put out of business when flooding of the area around their offices prevented access to their building. Although they had an off-site recovery plan, their only file backups were stored in the inaccessible computer room.

"Real disasters" are seldom obvious or direct; the World Trade Center bombing, the Loma Prieta Earthquake, the Hinsdale Central Office Fire, as profound as these events may have been, are but a small percentage of the 'disasters' facing the typical organization. The "typical" disaster is far more likely to look like the scenarios above. As often as not, they are compound failures gradually escalating from seemingly innocuous, recoverable glitches to near-tragedies. In most cases, human error (whether proactive or reactive, commission or omission) is the single greatest factor in growing a large headache into a small disaster.

How does one transform those large headaches into valuable learning experiences rather than into disasters?

Aggressively look for and address weaknesses in your contingency plans.

Use regular, structured walkthroughs or brainstorming sessions to isolate and resolve vulnerabilities.

Frequently test your contingency plans to failure: find the weakest links, rather than striving to demonstrate a successful recovery test.

Don't assume that "real" disasters will look like the scenarios you have tested: your contingency plan should address every conceivable disaster scenario, yet assume that the "real" disaster, which will be the ultimate test of the contingency plan, will be the one scenario which was not specifically considered.

=====

Copyright 1998, 2001, Rothstein Associates Inc. All Rights Reserved

=====

**go to [www.rothstein.com](http://www.rothstein.com)**

Philip Jan Rothstein, FBCI, President

[pjr@rothstein.com](mailto:pjr@rothstein.com)

Rothstein Associates Inc.

Management Consultants

¥ *Business Continuity, Disaster Recovery, Crisis Management*

¥ *Publishers of The Rothstein Catalog On Disaster Recovery:  
Hundreds of books, software tools, videos & research reports.*

[www.rothstein.com](http://www.rothstein.com)

[www.DisasterRecoveryBooks.com](http://www.DisasterRecoveryBooks.com)

[www.ServiceLevelBooks.com](http://www.ServiceLevelBooks.com)

203.740.7400 or 1-888-ROTHSTEIn fax 203.740.7401

4 Arapaho Rd. Brookfield, Connecticut 06804-3104 USA