The Newsletter of the Central New York Chapter of ARMA International

ARMAil
Central New York

Vol.16, No.1, October 2006

# Disasters Come in All Sizes

BY ROSALIE STREMPLE AND MICHAEL F. MARTONE

***Many disasters can be avoided – or at least their impact minimized – by taking the time to plan ahead***

A power outage knocks out a database server. A sprinkler system rains out a telemarketing office.A chemical spill from a tanker truck shuts down a nearby building. None of these are disasters in the usual sense of the word. But a company's ability to operate in these situations can be affected in ways similar to more commonly defined disasters.

Usually, disasters are thought of as large, newsworthy occurrences – earthquakes, hurricanes, floods, terrorist attacks. However, the most likely disaster for a company or organization is something small, such as computer software or hardware problems, telecommunications failure, or human error.

Preparing for a possible incident or disaster is usually viewed as advance preparation for effective *reaction* to an incident or disaster.However, an organization's contingency planning efforts should also be involved in the *proactive* mitigation of risks. The most effective way to minimize the adverse impact of an incident is to avoid the incident altogether.

## Risk Mitigation

Risks can be classified as threats that could cause an organization to be partially dysfunctional or result in total interruption of its normal operation. The disruption may result in anything from minor inconvenience to a full disaster.

The consequences of a disaster vary.They include loss of business, loss of productivity, and loss of data. Use of hot sites or cold sites can help resolve some of the issues. (A cold site is a site providing space for recovery of an impacted business process, a location that will require extensive effort before the business unit can use the space. A hot site is the most comprehensive alternate site; it has all the equipment,wiring,or special resources required for the business unit to function.) However, loss of data can have the greatest long-range impact following an incident.

Following are several possible ways to mitigate the risks associated with data lost due to disaster. While not intended to be all encompassing, the ideas presented may prompt thoughts of other ways to mitigate risks within an organization.

***Protection of centralized hardware is generally easier and less expensive to control than distributed systems, each with identical application software.***

**Power outage.** Because a power outage is one of the most common potential disasters, many organizations are aware of the dangers it poses. Some options to make an outage as transparent as possible include:

• **Provide one hour of uninterrupted power on all servers used internally.** Servers should be enabled with software that allows them to shut down gracefully, saving and/or backing up data as needed before the available power expires.

*Continued on page 3*

## 2006 - 2007 OFFICERS & DIRECTORS



**Solutions to CRM Corner -**
**1 - e**
**2 - b**
**3 - c no**
**4 - b**
**5 - b**

## *Message from the President, Patricia C. Franks*

An article in the September 11th issue of eWeek warned readers that securing systems is not enough. It's paramount to secure data regardless of the system used.

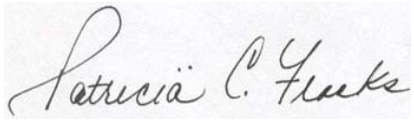
During the past few months, sensitive data stored on laptops have been compromised. Organizations that spend millions of dollars on security for their in-house information technology systems find themselves dealing with problems posed by employees with data stored on portable systems worth only a few thousand.

Of course, I'm sure the writer didn't mean that the systems should not be secure. But the focus should be on the data, regardless of the system used. That may sound like news to some, but it is an approach records managers take every day.

This year, CNYARMA's programs will focus on data in its various forms. Learn how to protect and recovery data in danger from both man-made and natural disasters by attending our first workshop on October 19, "A Document Recovery Primer." During our second program on December 7, find out how you can control your electronic documents by implementing an electronic document management system. To be sure we don't forget our paper records, we're planning a tour of a records center for March of 2007. Details on the tour will be announced on our website and in a future newsletter. And join us on May 31 to find out how you can mine your data to help you make sound business decisions.

One of the added benefits of attending CNYARMA programs is the opportunity to share ideas with your colleagues. Be sure to set those dates aside now. We're looking forward to meeting you in person very soon!

Sincerely,



Patricia C. Franks, Ph.D., CRM
CNYARMA President

## *CNYAMA Report of the Treasurer*

*Submitted by Edward L. Galvin, Treasurer*
*September 27, 2006*

| | |
|---|---|
| **Balance as of 4/11/06** | **$4656.65** |
| **INCOME:** | |
| Escrow (Membership) | $665.00 |
| June Sponsor | $300.00 |
| June Meeting | $410.00 |
| NE Region ARMA Meeting Refund | $ 50.00 |
| | **$1425.00** |
| **EXPENSES:** | |
| NE Region Leadership Meeting | $616.81 |
| June Meeting | $393.23 |
| Plaque for former secretary | $ 35.04 |
| ARMA International Conference | $799.00 |
| Flowers for departing secretary | $ 65.86 |
| Chapter Member of Year | $ 50.00 |
| | **$1959.94** |
| **Balance as of 9/27/06** | **$4121.71** |

• **Provide eight hours of uninterrupted power for all Web servers and required support hardware.** Depending on the nature of an organization and its business, it may be important to allow external users to get to the company's Web site.

• **Replace desktop systems with laptops where possible.** Laptops with built-in battery backup may allow users to continue working when power failure occurs in a building.

**Human error.** It is impossible to eliminate human error; however, train-ing can minimize it. Training also gives an organization a more empowered, proactive,andproblem-solving work-force. Approaches include:

• **Provide training for document versioning and encourage its use.** Document versioning software allows multiple users to review a requested revision, including deletions. The change must be accepted (possibly by multiple editors) prior to document revision.

• **Implement version control software.** Software is available that limits revision rights and provides the history of document revisions. This may be especially useful when dealing with documents revised on periodic schedules for release to targeted audiences, such as annual financial reports and student course offerings.

**Network failure.** Network failures may occur because of issues with power supply, servers, or software. The following actions can mitigate data loss due to network failure:

• **Enforce daily backups of both the servers and users' systems.**While the primary benefit of this is described below under hardware problems, a side benefit is that it may allow users to go back to previous versions of documents, reducing the scope of potential errors to one day at most.

• **Increase metering and monitoring of network usage.** A perceived network failure may actually be a failure of managing user expecta-tions. A technical challenge, which may not be possible, is to make consistent band-width available to allow access to applications, including Internet connectivity. It may not be possible to maximize both throughput and throughput consistency while offering users availability at top access speeds all day. Perceived difficulties connecting to network resources may be related more to bandwidth than to physical connections. One person listening to an Internet radio station can seriously impair productivity within an entire local area network (LAN). Existence and enforcement of information system policies should be designed to limit the non-business use of LAN resources.

**Hardware problems.** Housing data and software on a central server helps reduce the impact of individual work-station hardware failures Protection of centralized hardware is generally easier and less expensive to control than distributed systems, each with identical application software.To avoid potential hardware problems:

• **Consistently monitor users' systems.** Tools such as System ManagementServer, AssetWorks, NetCon, and Norton Desktop Administrator provide general baselines on PC performance to help identify problems before they become critical.

• **Reduce risk of users losing data from their own harddrives.** Al-though policy should strongly encourage users to store their data on secured servers, speed and availability issues ensure that at least some data will be stored on hard drives. Therefore, a combination of policy and technology is the best solution. Data stored on local drives should be stored in a C:\My Documents\ directory. While the desktop units are active (preferably during nonproduc- tion hours), batch files can scan and back up these directories on a regularly scheduled basis.

• **Reduce risk of damage to application servers.** All users should have access to at least two different server sources of the software applications at all times.Use of redundant arrays of inexpensive drives (RAID) provides some measure of uninterrupted service in the event of server hardware failure. A full list of the RAID levels is available at *www.nthelp.com/raidlev.htm*.

**Software malfunction including viruses and program bugs.** It is difficult to protect against program bugs. Software versions on user machines should be closely moni-tored.The most effective approach uses the same data versioning techni-ques described under "Human Error."
Alpha or Beta test software should be limited to test domains. System upgrades should be closely monitored. Other steps to minimize software malfunction include:

***Information is a corporate asset. Records containing information necessary to restore functions affected by an incident or disaster***

• **Purchase a virus protection program.** It is critical to purchase a virus protection program from a reputable company and include the software as part of any new system rollout. Encourage users to share straight-text messages rather than attachments where possible. Further, e-mailing of executables should be strongly discouraged. Executables are files that don't require other applications (such as Word or Excel) to run. Executables usually have an "exe"

*Continued on page 4*

extension. However, as extensions may not always be visible on the system, a good rule of thumb is to err on the side of caution until you have identified the origin and purpose of an attachment has been identified.

• **Enforce virus scans and updates.** The challenge with viruses is not in obtaining the needed software, but rather, enforcing the hard drive scans and the updates of the virus fingerprint files.Most major virus software packages allow both of these tasks to be scheduled in the background. Establish a policy to scan hard drives at least once a day.Most virus-scanning packages produce log files, which can be stored in a central repository and analyzed for trends.The systems administrator can produce compliance reports for upper management at regular intervals.

• **Ensure access to up-to-date virus information.** Rules about viruses change frequently. In the past, conventional wisdom lulled users into a mind-set that believed receiving an e-mail was safe as long as they did not open any associated attachment. However, viruses such as the Outlook Bubbleboy demonstrated that this is no longer the case.At least one person on staff must stay conversant with the many online forums that provide the latest in virus trends.

The most likely disaster for an organization is something small, such as computer problems, telecommunications, failure, or human error. Most businesses experience two hours of downtime per week. Thirty percent of computer users spend one week per year reconstructing lost data, according to a 3M study conducted in 1995.

| Incident | CFM Magazine (1997) | Ontrack | Disaster Recovery Journal |
|---|---|---|---|
| Power outages | 72.2% | | 31.1% |
| Computer hardware problems | 52.2% | 44% | |
| Telecommunication failures | 46.0% | | |
| Software problems/ computer viruses | 43.1% | 21% | |
| Human error | 34.4% | 32% | |
| Lightning storms | 33.7% | 3% (Natural disasters) | 20% (storm/huricane) |
| Floods | 16.8% | 3% (Natural disasters) | 16% (including burst pipes) |
| Fires and/or explosions | 14.1% | | 13% (fires/bombings) |
| Hurricanes | 12.5% | 3% (Natural disasters) | 20% (storm/hurricane) |
| Earthquakes | 9.1% | 3% (Natural disasters) | 9% |
| Violence (bombing/terrorism) | 7.3% | | 13% (fires/bombings) |

### The Role of the Records Manager

Information is a corporate asset. Records containing information necessary to restore functions affected by an incident or disaster must be protected. Other elements identified within business resumption plans may not be needed if the information required by the organization is not available. In a 1997 survey conducted by Hugh Smith of Firelock Data Protection Systems, the majority of records managers responding answered that risk management was not part of their job descriptions. Seventy percent answered that suggesting new or improved security for vital records was not their job. According to the same survey, those records managers stating that they were part of the disaster recovery planning process also had the tightest control throughout their organizations. The focus of a records and information manager is to ensure access to information at the right time, in the right place . During the business resumption planning process, the focus of data center management is to protect and restore electronic systems. Without involvement of a records manager, non-electronic forms of information may not be fully identified during the contingency planning process. As a member of the contingency planning/business recovery team, the records manager will have opportunities to interface with executive management, which might not be available in their information management program. By focusing attention on the interrelationship of information duplicated in multiple storage media, records managers can strengthen other components of their current program. Convincing management that records management is part of a larger security issue may help the program receive the respect – and the budget – it deserves.

### Keeping the Business "in Business"

The top five risks discussed here have one thing in common: They impact the users' ability to access or use information. A computer system difficulty that starts as a technical or operations issue can rapidly create crises in confidence, credibility, and good business relations. Therefore, business resumption/ contingency plans must address the potential for information loss. Records and information managers must help identify risks to which their organizations may be subject. Efforts to mitigate these risks may offer opportunities to strengthen overall information management practices. Developing plans to deal with keeping the business "in business" with alternate sources of vital information is central to all recovery plans. The leader of the RIM program should be involved in determining what to do to meet each type of emergency, should efforts to avert the incident fail.Without this type of involvement in reviewing, testing, and designing information recovery policies and procedures, opportunities to ensure the organization's understanding of information management versus information storage and processing are often missed.

## TEST YOUR PLAN BEFORE YOU NEED IT

Conducting a simulation exercise can point out the weaknesses of an organization's contingency plan so they can be strengthened prior to an actual disaster.Following is a guideline for conducting a simulation exercise:

**Determine the scope of the exercise.**The scope of the exercise should be designed to address apparent needs of the business or parts of the business participating in the exercise.These needs should be identified in conjunction with the appropriate staff. The scope may be designed to test the effectiveness of plans for recent additions to the organization or opportunities for improvements identified in previous tests or exercises.The scope:

- sets the course
- defines the playing field
- is designed to answer "big"questions

**Determine the timetable for the exercise.**

**Determine the teams and functions required to participate in the exercise.** Participants should be made aware of the scheduled simulation at least one month in advance.

**Determine measurable goals and objectives for the exercise.** Establishing the goals for the exercise promotes an understanding of what will be proven before beginning the exercise. Keep in mind that the simulation/test is not a pass/fail test; it is an exercise that illuminates ways to improve the plan. Objectives are the hinge upon which the exercise turns, and must be concise, measurable, and attainable.

Good objectives include:

- contact every level of the call tree successfully within one hour
- restore critical systems offsite within 48 hours
- evacuate the building and account for staff within 15 minutes
- contact key customers within one hour

Examples of bad objectives include:

- help the staff get back to work by finding and moving to another location as soon as possible (not concise or measurable)
- improve communication between line and support staff (not concise or measurable)
- restore every function within 48 hours in an off-site location (not attainable)

**Test methodology.** Notify participants in advance of the test.They should arrive at the test facility with documentation needed to facilitate their recovery (i.e., test plans, phone contacts, etc). The facilitator presents the ground rules for the session, including:

- A disaster scenario will be presented with some details. However, questions that team members may have about the situation will require further communication, just as in an actual incident. In the simulation, a method of capturing the give-and-take between participants must be used.
- A timeline for the exercise should be posted. For example, the actual clock may begin at 9 a.m., while the disaster clock may begin at 2 a.m.Updates may state the disaster time has progressed to 8 a.m., etc., without regard to the actual clock time.
- Updates to the situation should periodically be made available to participants. The updates can include new information, such asresponses given by other participants to questions having general impact Updates should simulate the increasing knowledge that will be available about the incident as the timeline extends.
- A method of tracking communicationbetween recovery teams must be established. Following an actual incident, communications would be fast and furious, ranging from telephone calls, faxes, and emails to face-to-face meetings and discussions. During the simulation, a method of capturing the details that will be exchanged must be used to allow incorporation of the resulting solutions into the planning process.Methods could include a standardized communication form, a central repository for e-mail messages, tape recordings, etc.
- The facilitator should prepare a summary report for participating teams and management concerning the outcome of the exercise.

**Plan improvements.** Lessons learned from the exercise must be incorporated into the recovery plans. Testing on a regular basis will allow the organization to build upon what it learns from each exercise. Regular testing will also identify changes in the business or its organization that may not have been included in previous versions of the in-effect recovery plan.

# The Value of Effective Disaster Recovery Planning

By Harold Hockman, Optical Image Technology, Inc.

Your organization is producing and saving more information than ever before. With the price of storage decreasing due to ongoing advances in technology, many businesses double their stored information every 18 months. Often this is a result of business initiatives, laws, and federal requirements that mandate that organizations retain specific information for a designated number of years. Industry rules often necessitate stringent reporting regulations to both regulatory agencies and customers, increasing the growth in retention requirements and data output.

Advances in technology have also driven the growth of information — and the subsequent need for storage — to enormous proportions. Where the previous industry standards included megabytes and gigabytes, storage reservoirs now boast the ability to hold terabytes and exabytes. As quantities grow and as regulations change, it becomes increasingly more difficult to determine what information should be preserved and what should be destroyed.

## CONTINGENCY PLANS

As business records accumulate, the obligation to manage and protect company escalates. This has been underscored by recent events that have brought the world's attention to the need for disaster recovery preparedness.

Terrorist acts, hurricanes, floods, blackouts, mudslides, and fires have forced businesses to look at their records in a new light. Companies are realizing that although paper files are extremely vulnerable to loss or damage, computerized files are equally susceptible.

Virus and worm attacks, as well as unforeseen network shutdowns, all have the capacity to grind business processes to a halt. But what constitutes an emergency? Disaster recovery means different things to different companies. For some, disaster recovery means protection against the accidental deletion or loss of files. Others anticipate man-made or natural disasters. Without access to their records, businesses could potentially suffer catastrophic losses from which they might never recover.

Recovery strategies are also essential because Sarbanes-Oxley (SOX), HIPAA, Gramm-Leach-Bliley, Check 21, and dozens of other regulations necessitate that companies institute thorough emergency preparedness plans. Regulators can impose harsh punishments and fines, and offer no latitude when a company is unable to meet requirements due to a disaster or other data-loss event. As businesses evaluate their contingency plans and prepare for emergencies, it is imperative that they place the highest priority on the integrity of their company records and perform regular database backups.

## BACKUPS vs. RECORD MANAGEMENT

Backup can be a complicated, intimidating process, whether it involves storing data on some form of removable storage medium, a secure offsite storage reservoir, or both,. Tapes are often cumbersome and disorganized. To complicate matters, administrators face difficulty in determining which information warrants backup. Often, a contingency plan involves making backup copies of everything. This expensive strategy can backfire in instances where federal regulations require deletion of sensitive information after a designated number of years. Redundancy is important; but it is also essential that disaster recovery backups involve a method of differentiating information which is mission critical from information that is less important.

To realize the greatest benefit from a backup and recovery strategy, it is vital for businesses to consider the life cycles of records, and which records have immediate relevancy to the business. The rationale behind this strategy is two-fold. By archiving less-relevant records on an inexpensive and slower medium, businesses can save money but still have access to older data. More importantly, this practice will facilitate increased access, and speed of access, to current records. During disaster recovery, large volumes of historical data can significantly delay the recovery process. Hours (or even days) could be lost while older, less important data is restored. For some companies, this delay can translate into millions of dollars. In terms of record life cycles, storage, archiving, retention, and destruction are factors worthy of consideration to avoid prolonging the recovery process. By storing current records on disk and other high-availability storage media, companies can ensure fast, immediate access and retrieval of relevant information. This information needs to be prioritized in advance to prepare for possible disaster recovery, ensuring lessdowntime after disaster strikes. Government- and industry-regulated retention and destruction schedules should also be implemented when considering a disaster recovery plan. By automating these schedules, businesses can ensure compliance with regulations that demand file retention or destruction. This practice also ensures that the volume of company records does not become unwieldy.

In a paper-based system, the records management component of disaster recovery can be a full-time job. Ensuring the safety and confidentiality of records is particularly difficult when one considers that there are more than 8000 state and federal regulations that affect records management. The best way to overcome this difficulty is to automate the process, which removes any potential for human error or inappropriate access to records.

Please visit DocFinity HSM as a Disaster Recovery Solution or call 814-238-0038 for information on how DocFinity® HSM helps with disaster recovery.

CRM corner

By Patricia C. Franks, Ph.D., CRM

Congratulations to all who passed the CRM exams this past May. As the CRM designation becomes more attractive to employers, more individuals working i in the records management field are working to earn this designation by taking and passing the 6-part exam. The first five parts are objective and the last is a case study. Below are examples of the kinds of questions you'll be asked if you take the first 5 parts. For more information about the Institute of Certified Records Managers or the CRM examination program, visit http://www.icrm.org.

Part I: Management Principles and the Records & Information Management Program

1. In the management decision-making process, which of the following is the initial step taken by a manager?
a. Developing alternatives.
b. Evaluating alternatives.
c. Choosing the best solution.
d. Implementing the decision.
e. None of the above.

Part 2: Records Creation and Use.

2. Informality, brevity, and low costs are the basic requirements of each of the following internal written communications media?
a. Reports.
b. Interoffice memoranda.
c. Written procedures.
d. Business letters.
e. Office manuals.

Part 3: Records Systems, Storage, and Retrieval.

3. Subject files are based on:
a. correspondent's name.
b. date of purchases.
c .topic of correspondence.
d. area of country.
e. all of the above.

Part 4: Records Appraisal, Retention, Protection, and Disposition

4. The process of evaluating the value of business records in the development of records retention schedules is known as:
a. accessioning.
b. appraisal.
c. disposition.
d. systems analysis.
e. scheduling.

Part 5: Facilities, Equipment, Supplies and Technology

5. Glass-like think tubes fine as human hair that send light from one location to another are:
a. microprocessors.
b. fiber optics.
c. lasers.
d. satellites.
e. narrowband carriers.

*answers to* CRM on page 2

**My Friends:**

**The next CNY ARMA luncheon meeting, "A Document Recovery Primer," will be held at the Holiday Inn, Cortland, NY on Thursday, October 19, 2006. The speaker is Joseph K. Perko, Account Manager, Document Recovery Services, Munters Corporation.**

**Joe will be discussing the categories of damage to texts; recovery and restorationa worst case scenario - Katrina; disaster recovery planning; funding disaster recovery: budgeting, FEMA, and grants.**
**The flyer has now been posted to the CNY ARMA website at http://archives.syr.edu/cnyarma/**

**Please print out and post or distribute to anyone who you may think will benefit from attending.**
**Deadline to sign up to attend is Monday, October 16! Call or e-mail Jackie Lewis at jlewis@herkimerarc.org or (315) 866-2920 to register.**

**If you would like to download the flyer directly just click on the link below.**
**http://archives.syr.edu/cnyarma/oct.pdf**

**CNY ARMA would like to thank Access Systems Consulting for their generous sposnsorship of our fall meeting.**

**If you have any difficulty reaching the documents, please let me know at elgalvin@syr.edu**

**Ed Galvin**
**Central New York ARMA Webmaster**

ARMAil
Central New York

# Meet your new best friend.

As the world's trusted leader in protecting, storing and managing business records, Iron Mountain offers an unrivaled choice of solutions that let you instantly access and retrieve records right from your desktop. Iron Mountain Connect™ is an innovative web-based tool that can reduce costs, increase control, and ensure ongoing compliance of your records management program. **To learn more about our wide range of products and services, call us at (800) 899-IRON or contact your Iron Mountain representative.**

IRON MOUNTAIN®

**www.ironmountain.com**

**RECORDS MANAGEMENT / SECURE SHREDDING / DIGITAL SERVICES / CONSULTING**