Disasters Come in All Sizes

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

BY ROSALIE STREMPLE AND MICHAEL F. MARTONE

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.

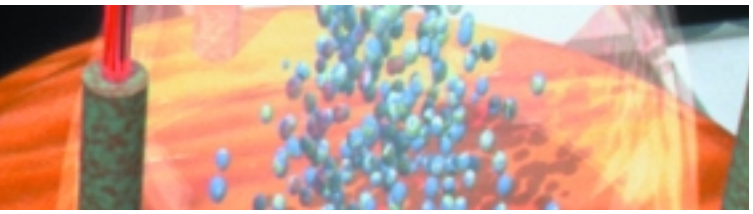
Preparing for a possible incident or disaster is usually viewed as advance preparation for effective *reaction* to an incident or disaster. However, an organization's contingency planning efforts should also be involved in the *proactive* mitigation of risks. The most effective way to minimize the adverse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

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



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.

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.
- 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, training can minimize it. Training also gives an organization a more empowered, proactive, and problem-solving workforce. 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 expectations. A technical challenge, which may not be possible, is to make consistent bandwidth 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 workstation 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 Management Server, 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 hard drives.** Although 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 non-production hours), batch files can scan and back up these directories on a regularly scheduled basis.

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

- **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 monitored. The most effective approach uses the same data versioning techniques 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:

- **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" 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 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.

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)

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 as responses 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 communication between recovery teams must be established. Following an actual incident, communications would be fast and furious, ranging from telephone calls, faxes, and e-mails 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.

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.

Rosalie Stremple is bank operations disaster recovery manager at Key Services Corporation, with headquarters in Cleveland, Ohio. She is currently pursuing a master's degree in management of information systems at Case Western Reserve University, Weatherhead School of Management in Cleveland. She can be reached at rosalie_c_stremple@keybank.com.

Michael F. Martone is the co-founder and vice president of operations for OddJobBid.Com (a Columbus-based labor auction service) and has co-written three books on technology certification. He can be reached at michael_martone@ yahoo.com.

Additional Resources

Additional information on disaster recovery is available at the following Web sites:

www.bmscat.com/

www.contingencyplanning.com/

www.system.missouri.edu/records/partc.html

www.drj.com/

www.alaska.net/~build/DISPLAN.HTM

www.disastercenter.com/displan.htm

www.rdiinc.com/english/plansde.htm

www.disaster-resource.com/

www.documentreprocessors.com/

www.rothstein.com/data1197/sx020004.htm

www.flooding.pl/

www.mnhs.org/prepast/conserve/recovery/recovery.html

www.ah.dcr.state.nc.us/archives/rec/plan.htm

www.ontrack.com/ao/ao.asp

www.panix.com/~vidipax/

www.rothstein.com/

http://turva.me.tut.fi/%7Eoshweb/

http://168.20.197.60/~tapp/osm405/chap9/index.htm

http://csn.uneb.edu/ProjectTeams/DisRecovery/index.html

http://alexia.lis.uiuc.edu/~johnpope/disaster_preparedness.html

http://lcweb.loc.gov/preserv/emerg/dry.html

http://spectre.ag.uiuc.edu/~disaster/guide/guide.html