Foundation NEWS & COMMENTARY
November/December 2001
Vol. 42, No. 6

BACK TO INDEX

COF HOME

DEPARTMENTS
At Issue
Feedback
Of All Things
Clips
Verbatim
Event
Reviews
Releases
People
Excerpt
Givers
FN&C Now

MORE ARTICLES
Government Update
Memorials
Web Sight

Technology

Emergency Preparedness

by Martin B. Schneiderman

Before September 11, the term *disaster* was commonly used to refer to large-scale natural events such as hurricanes, floods, tornados or earthquakes. Since then, there is heightened awareness that we are vulnerable in other ways, too. Consider the following reports of real-world emergencies that foundations and nonprofits have experienced in the past few years. Which of the following could happen to you?

Broken sprinkler. On a Saturday morning, a ceiling sprinkler activated on the floor above the offices of one foundation. By Monday, all server hardware and data tapes were destroyed. The foundation had no off-site backups. All data was lost.

ISP failure. One foundation was notified late on a Friday afternoon that its Internet service provider (ISP) had gone out of business. Its high-speed data line went dead that weekend. The foundation signed a contract with a new ISP a few days later, but it took more than a month for new service to be installed.

Brownouts. Intermittent power dips and outages caused one foundation's battery backup unit software to restart its servers improperly; the software had never been tested. The e-mail server's data was corrupted.

Power surge. A thunderstorm caused an electrical power surge. The battery back-up units didn't have effective surge protectors, so the circuits in the file servers and network hubs were "cooked." This was not covered by the manufacturer's warranty.

Fire. A building fire destroyed all the records of one foundation: its information systems, paper files and archives.

Water main break. A water main break occurred outside a multistory headquarters of one foundation. The fire department evacuated the building within a few hours because the sprinklers couldn't operate. All building access was denied for days.

Virus attack. All desktop computers and servers at one foundation had antivirus software installed and running. A program officer opened an e-

Foundation News & Commentary is published by the Council on Foundations, 1828 L Street, NW, Washington, DC 20036, 202/466-6512 Fax 202/785-3926
Chair
William C. Richardson
President and CEO
Dorothy S. Ridings
Vice President, Constituent Relations Group
Sunshine Janda Overkamp
The Council on Foundations is a membership organization that serves the public good by promoting and enhancing responsible and effective philanthropy. Foundation News & Commentary embodies and promotes the goals of the Council on Foundations, serving as a vehicle for information, ideas, analysis and commentary relevant to effective grantmaking. It seeks to enhance understanding of organized philanthropy by grantseekers, policymakers, opinion leaders and the society at large, but it is directed primarily toward the trustees and staff of donor organizations.

mail message with an infected file attachment, unleashing a virulent virus into her computer and the foundation's file server. It corrupted all e-mail accounts and deleted thousands of data files. Then, the foundation discovered its antivirus software signatures had not been configured to update properly—they were more than six months out of date.

Web site update. One community foundation, unable to update its Web site immediately after a regional disaster, could not advise the public how relief was being provided—nobody on staff had the necessary Web expertise. The foundation turned to its grants management software provider to step in and get the job done.

Hacker attack. Many organizations have had their Web sites hacked and defaced with profanities. Others have experienced Denial of Service (DoS) attacks—where hackers send a flood of traffic at a network router, seriously disrupting or preventing Internet access.

Blank back-ups. An inexperienced part-time network administrator had been following step-by-step instructions to make daily server back-ups. After accidentally erasing data directories on the server, he attempted to restore the files from a back-up tape. That's when he discovered that none of the back-up tapes contained any data. No one had ever checked the back-up logs. Nor had anyone ever attempted to restore a file from a back-up tape as a test.

No documentation. One nonprofit's self-taught network administrator left to take a new job. Nobody was hired to replace him. A month later, the office experienced a system failure. There was no system documentation and nobody knew all of the login IDs or passwords. With the help of a consultant, all systems were eventually restored. However, it took weeks longer than it should have to do the job, because the network had been configured in a very "nonstandard" way.

Access denied. One family foundation's HR director was the only person who had the password to its custom payroll system. Unfortunately, she became very sick and went into a coma. Back at the office, nobody could access the system to process the month-end payroll.

Flood. One nonprofit organization's back-up tapes were stored two blocks away in a local bank vault. A flood caused the evacuation of the entire downtown, including where the nonprofit's office was located. The group's staff had the foresight to set up spare workstations and a server in another location for use in an emergency. However, there was one catch: The bank, too, was inaccessible. Data could not be retrieved from either the office or the bank vault for more than a week.

World Trade Center attack. The offices of two foundations were destroyed when the twin towers were attacked, and neither had back-up tapes off site. Both foundations were able to restore older grant data from back-ups that they had previously sent to their grants management software provider. In addition, many organizations throughout Manhattan experienced phone and data outages for weeks after September 11.

Minimize Your Risk

The September 11 attacks have motivated some organizations to take another look at their own preparedness. Here's a checklist of some ways to prevent problems from happening, to minimize loss when they do and to

speed recovery to normal working conditions:

- ***Test a realistic emergency management plan.*** Check out **www.fema. gov/library**—Federal Emergency Management Agency (FEMA) Virtual Library—and **www.fema.gov/library/bizindex.htm**—Emergency Management Guide for Business & Industry.
- ***Maintain detailed, up-to-date system documentation.*** Make sure that this is a staff member's responsibility and it gets done. Documentation should include lists of all key technical contacts, service providers, system passwords and your system configuration. Store it in a secure location that can be readily accessed by key staff in an emergency.
- ***Cross-train staff.*** Depending on a single person's knowledge is a risk no organization should take.
- ***Locate your servers*** in a secured area.
- ***Store all vital data on servers***, not on workstations.
- ***Provide remote access to office systems*** so that staff can work from home offices ("How to Quit the Commute," Foundation News & Commentary, September/October 2001).
- ***Consider contracting with a grants management Application Service Provider (ASP)*** to provide hosting services that can be accessed via a Web browser from multiple locations. Bromelkamp, CyberGrants, Digital Footbridge, MicroEdge and NPO Solutions all offer this alternative.
- ***Install uninterruptible power supplies (UPS)*** with built-in surge protectors on all servers, network communications devices, firewalls and telephone switches. Configure and test the associated software of your UPS to ensure it can execute an automatic, orderly shutdown of all servers should a power failure occur. Replace your UPS' batteries every 36 months.
- ***Install automated monitoring and alerting systems*** to constantly measure your computer room's temperature, humidity and flow of electricity and to notify you immediately when there's a problem.
- ***Install and maintain a top-rated hardware firewall at headquarters*** and software firewalls on all laptop and home-office computers. Review logs regularly to identify attempted breaches and intrusions.
- ***Install and configure virus detection software*** to be operating at all times on all computing devices. Ensure that the latest virus signatures are updated at least weekly on all computers. It's best to configure the software to do this without user intervention—if you expect your staff to do this individually, it just won't happen.
- ***Devise a tape back-up scheme that makes sense for your organization.*** Ensure that all data files, including open database files, are backed up daily and stored in a secure waterproof and fireproof media safe. Make certain that your back-up plan can restore the complete system. At least store month-end tapes off site, outside of your "threat zone," preferably in a secured facility with 24/7 access.
- ***Clean tape drives regularly*** and replace tapes according to the manufacturer's recommendations.
- ***Prevent "single points of failure" whenever possible.*** Maintain a spare part inventory for individual components, especially in critical systems. Consider a maintenance contract on extremely expensive or complex equipment. Read the service-level agreement carefully, preferably with legal review.

- ***Don't put all of your communications "eggs" in one basket.*** If available, consider installing multiple redundant lines from different carriers that are routed through different switching offices.
- ***Use cell phones as back-ups.***
- ***Maintain free Web-based e-mail accounts***—such as those offered by Yahoo! or Hotmail—as back-ups.
- ***Periodically review your insurance policy*** to see what's covered and what's not.

Overall, it helps to remember the scouting motto: "Be prepared."

---

*Martin B. Schneiderman is president of Information Age Associates, Inc., (**www.iaa.com**), a firm specializing in the design, management, and support of information systems for grantmakers and nonprofits. He can be reached at **mbs@iaa.com**.*

Back to Index