

Business Continuity Planning in Times of Change and Disaster

Moderator:

Richard Kobel

American Institute of Physics
Melville, New York

Speakers:

Denis Baskin

*Journal of Histochemistry and
Cytochemistry*
Seattle, Washington

James Wonder

American Institute of Physics
Melville, New York

Richard W Newman

American Medical Association
Chicago, Illinois

Reporter:

Jamie Holaday

Blackbaud
Charleston, South Carolina

No one has yet forgotten the 2005 bombings in London. Nor has anyone in the publishing community forgotten its effect on the *BMJ*, whose offices are near the location of one of the blasts. The journal had a plan, and its staff were able to continue working despite being denied access to their building.

Using the *BMJ* as an example, Denis Baskin and Richard Newman reminded us that being prepared in case something like this happens again does not require a high-technology solution. It may not be a bombing that interrupts work; disasters can include fire, a regional natural disaster, vandalism or theft, power failures, pandemics, or even disruptions in nearby offices, such as a crime scene on another floor of the building. No matter what the nature of the emergency, it's important that the work of the journal continue. Furthermore, as Newman pointed out, in the United States, the Occupational

Safety and Health Act requires employers to maintain emergency plans.

At the *Journal of Histochemistry and Cytochemistry*, Baskin started by making an inventory of the journal's business components. They can include vendors, contractors, offices, and affiliated organizations. Baskin then set priorities among items that needed to be protected, such as financial records, the subscription database, manuscripts, the reviewer and author database, servers, and personnel records. Next, staff members were assigned responsibility for each item. Test plans have been put on paper, and regular drills are performed to test and perfect them.

In a similar manner, Newman described how the American Medical Association (AMA) concentrates on emergency management and protecting people first. Its plan includes a Web site to post the current operating status of the organization and an evacuation plan that includes rally points. All employees are issued an emergency-contact card that lists contact information and rallying points. Certain employees are designated as floor leaders, who are responsible for particular subsets of co-workers. A floor leader is also in charge of an emergency kit containing essentials, including a list of employees who should be present.

Newman recommends that organizations that want to get started in creating continuity plans look to such organizations as the Federal Emergency Management Agency, the American Red Cross, the Institute for Business & Home Safety, and the Public Entity Risk Institute for tips. If an organization has no current plan, Newman suggests that a good way to start is to assemble contact lists for employees, key vendors, and key customers.

Both Newman and Baskin suggested working with vendors to investigate their continuity plans. Some vendors may also be able to help in the event of a disaster.

For example, the AMA has an agreement with Hyatt Hotels to use their facilities for office space in case its offices become unavailable.

On a larger scale, James Wonder spoke about how the American Institute of Physics (AIP) prepares for disasters as a service provider for more than 100 journals. Its servers need to be up and running 24 hours a day. In 1999, disaster planning began in earnest, and AIP partnered with IBM to ensure that IBM could get the servers operating within 72 hours of a disaster; this can include providing trailers in AIP's parking lot to create ad hoc office space.

In 2002, AIP went a step further and created a duplicate site, complete with servers and all the same software and equipment. The second site is 20 miles away, and AIP would lose only 2 to 3 seconds of data if it needs to transfer services. The duplicate site has been used three times in practice scenarios and has performed well.

To help to prevent problems in the first place, AIP contracts monitoring services that watch the system and look for abnormalities and potential problems. That allows AIP to act preemptively. 