innovative
a ProQuest Company

Planning for a Disaster: What Librarians Should Know

As the coronavirus outbreak has shown, libraries of all sizes and in all areas of the country need to be prepared for any contingency.

Librarians should take steps to protect their assets and should know what to do in the event of a fire, flood, earthquake, storm, riot, cyber attack, pandemic, or other emergency. Proper planning can help mitigate any damage and can aid in recovery, allowing patrons to have access to essential services with minimal disruption.

Disaster planning should address the safety of all people (patrons and library staff) and the preservation of all collections, including physical materials and electronic databases and information. An effective strategy should encompass three phases: preparation, response, and recovery—or what to do before, during, and after a crisis occurs.

This white paper suggests important aspects to consider when putting together a disaster plan, and it offers resources for further exploration.

Preparation

The key to getting through a crisis successfully is to be well prepared in advance. Here are some of the things you can do to ensure that your libraries are fully prepared to handle any eventuality.

BEGIN WITH A RISK ASSESSMENT. To prepare effectively, it's important to know how your institution is most vulnerable to a disaster, says Miriam Centeno, preservation and digitization strategist for The Ohio State University Libraries. For instance: Do your assets have to be stored within a certain temperature or humidity range? Is your HVAC system reliable? Does your location have a history of earthquakes, storms, or floods? Does your facility have a history of water leaks or mold?

Centeno suggests that leaders partner with preservation specialists and facilities managers to conduct a thorough risk assessment. *"This shouldn't happen in isolation,"* she says of the process.

MAKE SURE ALL ASSETS ARE FULLY INSURED. If assets that are damaged can't be restored or repaired, you'll want to recover the replacement cost of those items. Take photos of important assets, so you have a record of their condition before a disaster occurs.

COLLECT WHAT YOU'LL NEED IN THE EVENT OF AN EMERGENCY. When disaster strikes, you don't want to have to scramble around, trying to find the items you need to respond effectively. Assemble these items in advance and store them in a safe place, ideally in multiple locations both on- and offsite. Here are some of the things you should pull together, although this list is not meant to be comprehensive[1]:

DISASTER CONTACTS

The contact information for anyone you might need to reach in an emergency, including internal stakeholders such as board members, department heads, and disaster response teams, as well as police, fire, plumbers, electricians, locksmiths, utilities, insurance, and people with important institutional knowledge of your facility and its assets.

EMERGENCY INFORMATION

Emergency response supplies, such as information about water, gas, and electrical shutoffs, as well as keys, fire extinguishers, radios, and first aid kits.

CATALOG

Lists of all of your physical and electronic assets, along with information about where these items are stored.

RESPONSE KITS

Supplies for salvaging books and other collections. Centeno and her colleagues have put together disaster response kits for the Ohio State University Libraries, and these kits are located strategically throughout each library facility. They contain essential supplies to help employees respond to a variety of emergencies, such as plastic sheeting to cover assets in the event of a water leak and water containment pillows to divert the flow of water away from collections.

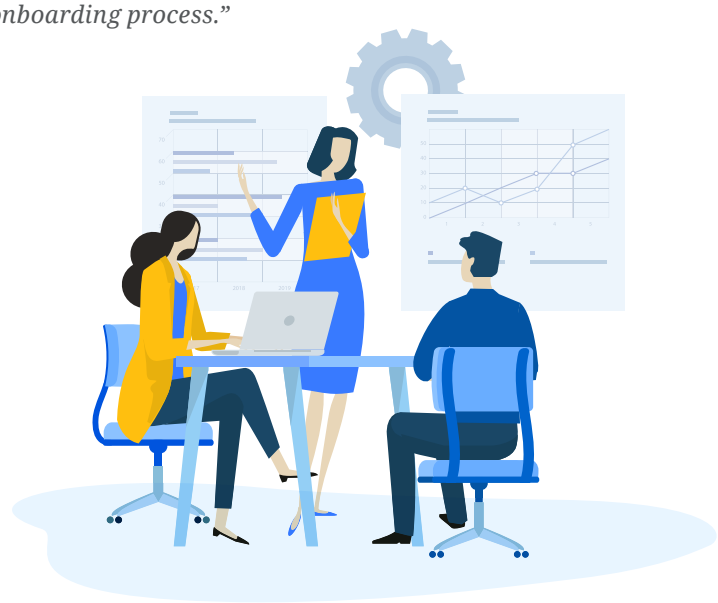
ASSIGN ROLES. All employees should know how to respond during a crisis situation. Assigning specific roles or responsibilities to each staff member can help you make sure that all necessary steps are accounted for and can reduce the likelihood of chaos that a disaster might produce.

Centeno recommends that libraries create a command team that is responsible for disaster planning and a response team that is mobilized in the event of an emergency. She suggests that libraries follow the Incident Command System (ICS) established by the Federal Emergency Management Agency (FEMA), so that leaders understand who should be on each disaster team, what roles they should occupy, and how they should communicate in the event of a disaster. FEMA offers an online ICS training and certification course that personnel can take to learn the system.

PRACTICE. As with anything else, practicing for an emergency situation leads to improvement in your response. Don't wait for a disaster to occur before applying roles and responsibilities for the first time; instead, hold drills, simulations, and tabletop exercises on a regular basis. The more effectively you can train staff to respond properly to any disaster, the more you can trust each other to respond safely and efficiently.

Martha Horan, head of preservation strategies for the University of Miami Libraries, says that disaster planning, preparation, and rehearsal should become ongoing activities and not simply a once-a-year exercise.

"Ongoing thinking about disasters allows us to keep these in our collective consciousness and be prepared," she says. *"It can be easy to forget if it's something you only think about once per year. A lot of changes can occur in a year, with shifts in staff and roles. Staff need to know where to find the right information, what the procedures are, and who to contact. New staff need to know this information, and it should be part of the onboarding process."*



PLAN FOR REMOTE ACCESS. Think about how patrons might continue to access library resources if they can't visit a physical location. The coronavirus pandemic has show the value of offering ebooks and electronic databases in addition to print-based materials.

It's not just patrons who need remote access to library resources; library staff need remote access to administrative systems, and facilities staff need a way to monitor and control the temperature, humidity, and ventilation of buildings remotely in order to maintain a proper environment even if they can't have physically access.

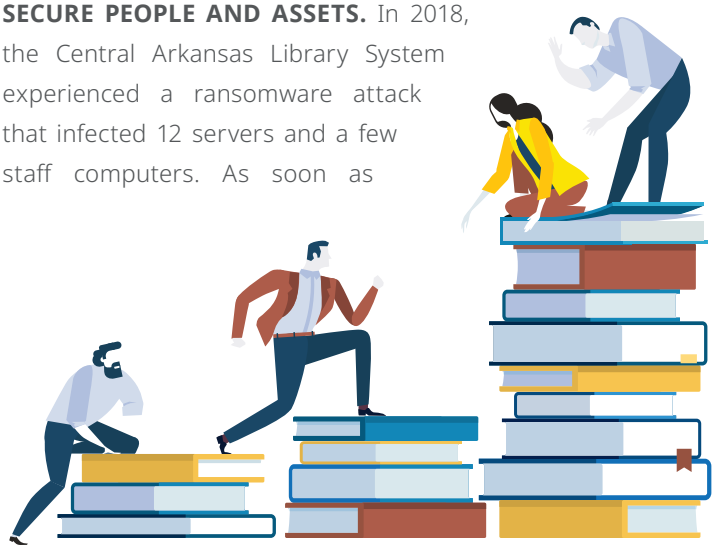
BACK UP ALL ELECTRONIC SYSTEMS OFFSITE. Backing up your data to the cloud ensures that you can recover lost information if anything should happen to your physical servers. Another option is to move information systems entirely to the cloud, rather than hosting them locally.

New Orleans Public Library maintained its integrated library system (ILS) software on a server in the basement of its main branch until 2018, when the library migrated to the Polaris ILS with cloud hosting services. *"Now, with hosted services, we won't need to wait for a site restore (if anything should happen to our libraries),"* says IT Director Jerry Pinkston. *"We can rest assured that our patron data is secure, and when we experience another weather-related event, we'll be ready to operate as soon as the building is open to patrons."*

Response

Planning for any contingency helps libraries react swiftly and decisively in the event of a crisis. Here are two critical actions to take if a disaster should occur.

SECURE PEOPLE AND ASSETS. In 2018, the Central Arkansas Library System experienced a ransomware attack that infected 12 servers and a few staff computers. As soon as officials discovered the attack, they immediately disconnected all the machines on that segment of the network to prevent any further breach of information.



Nathan James, deputy executive director of technology and collection innovation for the library system, compares this action to "shutting off the water in the event of a leak."

When disaster strikes, library staff should do what they can to make sure other employees and visitors are safe—and then take steps to avoid any additional loss or damage to the library's assets. Depending on the nature of the incident, this might involve containing a flood or fire, removing compromised information systems from the network, or transferring collections to a secure location.

COMMUNICATE REGULARLY. It's important to keep stakeholders informed throughout the crisis. *"Determining who needs to know is essential,"* James says. When the Central Arkansas Library System learned of the attack on its network, *"we immediately let our board of directors know,"* he says. *"We also sent out a statement to our staff that night with the information we had at the time."*

When putting out information, present only the facts that you know; don't make any assumptions. You must be open and transparent, but you don't want to cause panic. Issue regular updates as the situation evolves or as new information becomes available, so stakeholders aren't kept in the dark.

Recovery

Once the immediate threat is over, it's time to shift into the recovery phase, which involves assessing the damage and working to restore or replace materials. Here are some suggestions to guide you.

WORK WITH RECOVERY SPECIALISTS. Assessing the extent of the damage *"can be difficult without expert help,"* James says. *"I don't know what we would have done without expert help."*

When James and his colleagues discovered the cyber security breach, one of their first calls was to their insurance company, which connected them with a ransomware recovery specialist. The specialist helped the Central Arkansas Library System identify all compromised files, resolve the attack, and recover lost systems.

DOCUMENT EVERYTHING. Keep careful records of all aspects of the recovery process—including damages, expenses, copies

of written communications, and even time and services donated. *"You're going to need this information for legal reasons and insurance purposes,"* James observes.

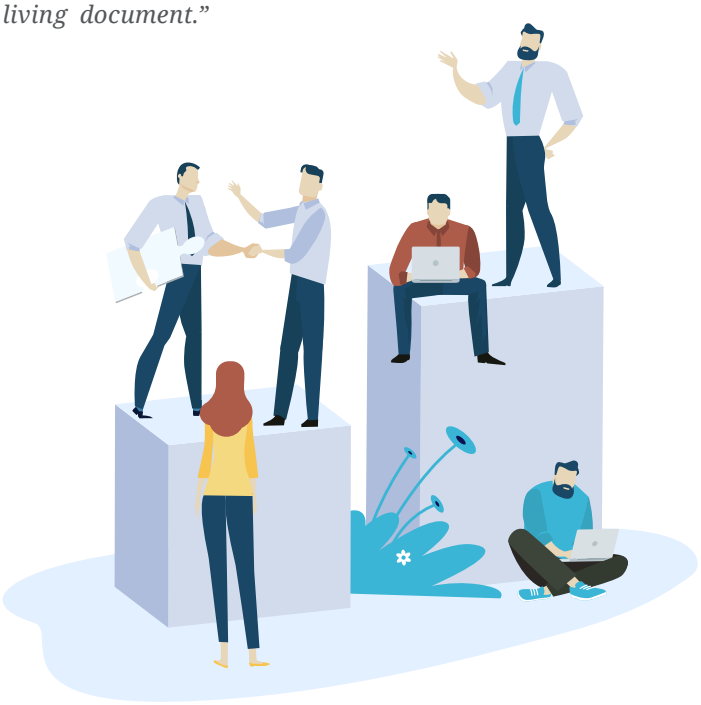
EXPLORE GRANTS AND OTHER RESOURCES THAT CAN HELP. Libraries might qualify for federal funding to help with disaster response and recovery. For instance, the National Endowment for the Humanities (NEH) Preservation Assistance Grants help small and mid-sized institutions improve their ability to preserve and care for their humanities collections.

Libraries can also contact the National Heritage Responders (NHR) for help in a disaster. NHR is a group of conservators, archivists, collection managers, and other professionals with skills and experience in handling a wide range of materials. They respond to the needs of cultural institutions during emergencies.

Be Prepared

Planning effectively for any situation can help libraries save lives, preserve assets, and restore essential services as quickly as possible should a disaster occur.

"It takes work to maintain a disaster plan, and the planning process needs support on different levels," Horan concludes. *"This requires building relationships with various departments across the institution. It's easy for disaster planning and preparation to become a lower priority—until suddenly it's not. From our perspective, a disaster plan must be a living document."*



innovative
a ProQuest Company

FOR MORE INFORMATION, CONSULT THE FOLLOWING RESOURCES:

American Library Association: Disaster Preparedness and Recovery
http://www.ala.org/advocacy/disaster-preparedness

ALA Disaster Preparedness LibGuide
https://libguides.ala.org/disaster/preparedness

Council of State Archivists: Pocket Response Plan™ Templates
The Pocket Response Plan (PReP) is a concise document for recording essential information needed by staff in case of a disaster or other emergency. Every person having a response-related assignment should carry a PReP with them at all times.
https://www.statearchivists.org/programs/emergency-preparedness/emergency-preparedness-resources/pocket-response-plantm-prep-tm-english-template/

FEMA: Incident Command System (ICS) Training
https://training.fema.gov/is/courseoverview.aspx?code=IS-100.c

National Heritage Responders
(202) 661-8068
http://www.conservation-us.org/resources/emergencies/national-heritage-responders

Applying for NEH Preservation Assistance Grants
https://www.connectingtocollections.org/recording-community-webinar-applying-to-nehs-preservation-assistance-grants/

Cyber Security for Libraries:
How to Prepare for a Ransomware Attack
https://vimeopro.com/innovativeiii/webinars/video/379299422

[1] This list was adapted from Amigos Library Services' "A Disaster Plan for Libraries and Archives," retrieved from https://www.amigos.org/sites/default/files/disasterplan_template.pdf.