IT Crisis Preparedness Countdown

Guidelines for establishing an IT emergency operations plan.

From The Consortium for School Networking

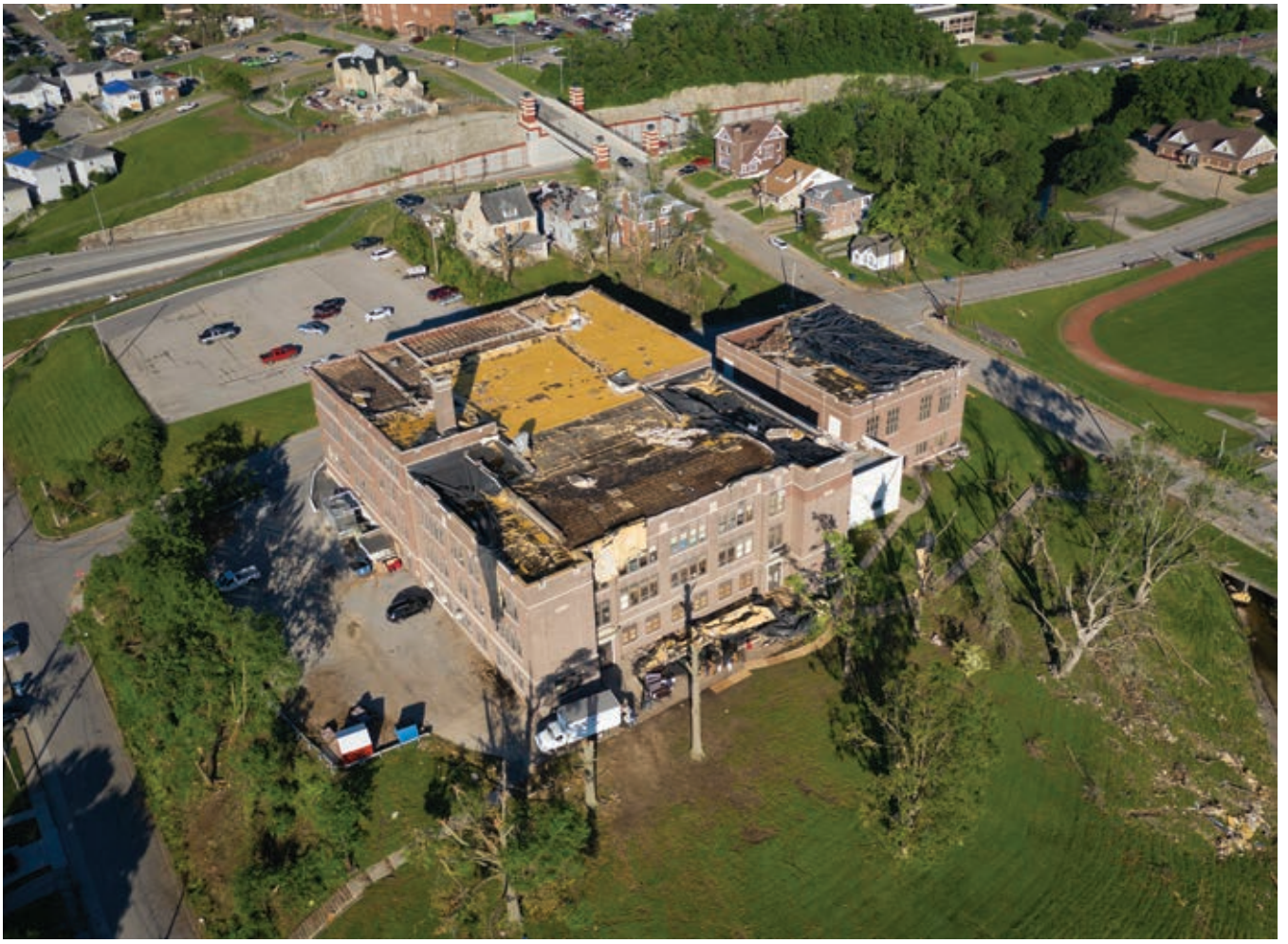


PHOTO BY NOTLEY HAWKINS, WWW.NOTLEYHAWKINS.COM

Regardless of geographical location, school district IT personnel must engage in emergency operations planning. Hurricanes, earthquakes, fires, tornados, and ice storms are just a few of the disasters that can impact technology operations.

Before a disaster hits, districts must be prepared to assess the damage, bring critical systems back online, update stakeholders, and resume operations as quickly as possible. A carefully considered IT continuity plan, as part of a larger emergency operations plan, is critical for school systems.

General Disaster Preparedness

The Readiness and Emergency Management for Schools Technical Assistance Center (REMS TA) of the U. S. Department of Education (https://rems.ed.gov) provides in-depth emergency operations planning (EOP) resources for schools.

IT crisis preparedness is an important component of any EOP. All school systems should develop an emergency operations plan that includes clearly defined roles and responsibilities for emergency response teams, including IT personnel.

TIME TO STORM	ACTIONS
72 Hours	• Confirm teams to perform post-storm site visits. • Ensure teams have the necessary equipment, such as masks, boots, and flashlights. • Provide each team with a digital camera to take time- and date-stamped photos after the storm, since cellphone cameras don't always offer this functionality.
48 Hours	• Confirm the primary point of contact for each facility. • Confirm that key network and hardware vendors have replacement equipment readily available to expedite post-storm replacement if needed. • Sign necessary forms allowing vendors to ship replacement equipment immediately without going through the regular purchase order process. Policies should be flexible enough to allow for the timely replacement of damaged equipment, but require documentation so as to assure the integrity of the purchase process and meet FEMA and insurance requirements. • Track the number of hours being worked by emergency personnel so as to apply for FEMA reimbursement. • Confirm who needs to receive technology status information post-storm and the appropriate format for transmission. • Ensure command center has multiple copies of district maps to assist with the deployment of assessment crews.
24 Hours	• Have employees unplug their computers and raise them off the floor when possible. • Physically protect network equipment when possible. • Shut down low-priority systems. • Allow individuals who will be working on site during the event to go home and make necessary preparations. • Gather EOP personnel at the command center. Ensure there are adequate personnel support resources, including food, water, and bedding.

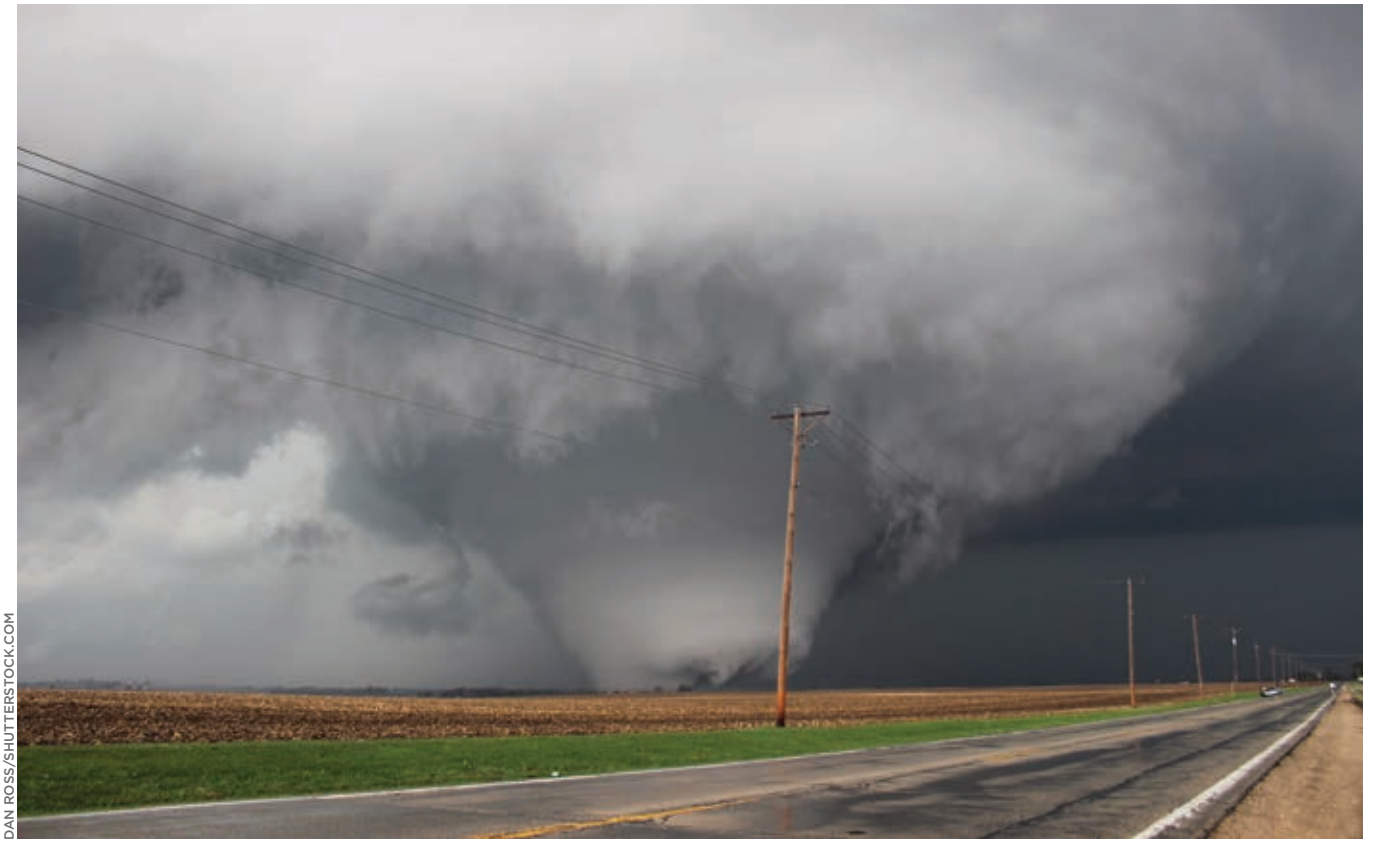
- Consider the potential disruption of regular communication methods when developing communication plans and protocols for before, during, and after the disaster.
- Define what information will be communicated and by whom to ensure that only accurate information is being given.
- Set up conference bridges in advance and share the information with the appropriate teams: cabinet, IT, etc.
- Ensure that wireless hotspots are available for emergency response personnel.
- Develop post-disaster assessment resources, such as damage identification and evaluation templates.
- Establish baseline criteria to determine when schools are ready to re-open.
- Consider developing board-approved emergency purchase waivers that allow district personnel to expedite the repair and/or replacement of damaged IT equipment and facilities in case of a disaster. Waivers should be reviewed by district legal counsel.
- Have vendor agreements in place with companies outside the immediate geographical area who are not likely to be affected by the same disaster, including IT and facilities vendors.
- Review FEMA regulations on an annual basis. Work with the agency and local government agencies to do annual regulation reviews, as regulations change frequently.
- Consider getting Government Emergency Telecommunication Service cards for board members and members of the district emergency operations team (www.dhs.gov/cisa/government-emergency-telecommunications-service-gets).
- Document and take pictures of IT facilities and equipment for FEMA and insurance purposes.
- Consider purchasing backup generators for key locations, such as data centers or emergency command locations.
- Back up key systems such as payroll and finance off site and determine how financial payments will be made after the disaster. Determine how critical IT systems will be restored in the event that onsite infrastructure is destroyed or inaccessible.
- Ensure that entertainment options are available for people manning the command center during downtime.

Preparing with Advance Warning

For natural disasters for which there is advance warning, such as with hurricanes, districts should create a checklist of actions to be taken 72, 48, and 24 hours before the storm.

During the Disaster

During the disaster, monitor network power and disaster status from a secure location. Begin to triage the remediation in affected areas.



DAN ROSS/SHUTTERSTOCK.COM

After the Disaster

- Allow extra travel time to affected sites due to their potential accessibility. Determine the safest routes of travel and availability of fuel.
- Have facilities teams inspect buildings for structural soundness and air quality before allowing employees to enter buildings.
- Deploy technology assessment teams as soon as it is safe to do so.
- Have assessment team leads collect and report information about conditions at each site.
- Ensure damage assessment information is collected in a centralized location.
- Prioritize the repair of critical technology systems such as payroll and finance.
- Determine if cell phone service is widely available in the local area. Communication outages may be short in some areas but may last weeks in others.
- Communicate regularly with board members.
- Bring in counselors to help students and staff deal with the event and its aftermath.
- Leverage the district website to communicate repair status, school closures, and other pertinent information. The website should be redirected to a location that can handle higher traffic and is not dependent on local infrastructure.
- Limit press communications to official channels to ensure the accuracy of data made available to the public.
- Establish official channels through which community members can donate funds or otherwise assist with recovery.
- Track the status of equipment replacement and repairs at each campus.

Evaluating Lessons Learned

After the event, identify lessons learned and incorporate into future IT crisis preparation plans. This important activity should be done in two stages:

1. After the immediate crisis has passed, evaluate the emergency response from an IT department perspective while problems are fresh in everyone's mind. Other operational units should conduct their own emergency response evaluations to determine areas for improvement.
2. Soon thereafter, conduct a districtwide post-mortem with cabinet and emergency staff. Adjust emergency procedures as needed based on the evaluations done by each operational unit.

Reprinted with permission from the Consortium for School Networking. www.cosn.org. Find additional IT crisis preparedness/disaster recovery resources at www.cosn.org/focus-areas/it-management/send-smart-education-networks-design/it-crisis-preparedness