At the Ready: Planning for Business Continuity

School system leaders never know when disaster may strike. Having a plan in place to protect vital data and systems is crucial.

By Linda Sharp

Floods in Indiana. Tornadoes in Louisiana. Blizzards in the Northeast. A shooting in Colorado. An H1N1 flu pandemic nationwide.

These headline topics of the past year are a reminder that schools and school systems across the country can be disrupted at any time. Thus, school system leaders need to be actively involved in crisis preparedness, planned response, and recovery to ensure student and staff safety and to make certain that all important operations, services, processes, and facilities continue to function in a disaster or crisis.

Planning for a Crisis

Planning is critical in the crisis preparedness process. The first step is to form a crisis preparedness team that includes members from the administration, technology department, custodial staff, personnel office, and community partners, such as the fire and police departments. This team is charged with identifying potential threats, developing and communicating the crisis preparedness plan, and putting the processes in place in case of a disaster.

The team should identify all potential threats, remembering that although their schools may not lie in the path of a hurricane or potential wildfire, natural disasters are only a fraction of the situations they must plan for. In the past year, as illustrated by the headlines, schools have experienced pandemics, shootings, building fires, and floods.

> The team must take time to identify all potential problems within the school or district's technology infrastructure.

The team should also focus on technology and its role in ensuring that the district can conduct business. Technology plays a critical role in instructional activities, data and record keeping, assessment and accountability, and internal and external communication with stakeholders. To develop a comprehensive plan, the team must take time to identify all potential problems within the school or district's technology infrastructure.

After the team has identified possible threats, members can begin to develop a complete a comprehensive plan, taking into consideration the personnel, facilities, hardware, software, and communication resources that are critical to the daily business of the school district. For example, they should prioritize which systems should be protected first. Protecting the server that houses all the district financial records is more critical than protecting the library server.

Mitigation, Response, and Recovery

Next, the team should develop a mitigation plan. Mitigation is the action taken to identify preventable and unavoidable disasters and to address what can be done to eliminate or reduce the likelihood of a disaster and its accompanying risks. The mitigation plan should

- Ensure student and personnel information is clean and up-to-date so you can notify all students and staff of a problem at school.
- Clearly label all rooms in all buildings with room numbers inside and out and practice evacuation drills routinely.
- Ensure all servers are protected from physical disruptions, such as water damage and tampering, and are routinely backed up.

These are just a few examples of issues the mitigation plan should address to ensure the plan will be successful and unexpected problems can be identified in advance.

Think through all processes, people, and procedures to guarantee that your district is prepared.

Response—the execution of the preparedness plan—and recovery—the efficient and timely restoration of mission-critical operations and processes—determine how quickly business can return to normal, which is your goal.

The Consortium for School Networking (CoSN) developed a 10-step information technology recovery process that may be helpful to schools and school systems:

1. Identify and contact personnel in charge of recovery efforts. Establishing communications with recovery leaders is critical. These individuals can be at the school, district, or state level and may include the superintendent (or liaison), technology leaders, public relations staff, human resources and maintenance personnel, and police and fire department representatives. These individuals may not normally be at the executive level, but all will be needed during recovery.

   Tip: Keep track of all hours worked by you and your staff. The Federal Emergency Management Agency (FEMA) will compensate personnel for wages that are not covered by the district.

KEY TIPS FOR CRISIS PLANNING

- During the planning process, fully inventory your assets annually so you can file insurance claims accurately and with documentation.
- Ensure that your technology department backs up important data off-site and can restore the data if necessary.
- Be sure that you and your community partners have blueprints of all buildings with clearly labeled room numbers, shutoff valves, and known hazard areas. Identify evacuation sites and procedures for communicating with personnel during a crisis.
- Establish a process to notify staff and students in an emergency during the school day and in off-hours.
- Identify the spokesperson (and backup) who will be responsible for dealing with the public and press. Stress to the staff that they are not authorized to speak for the school and should refer all inquiries to your spokesperson.

2. Identify or establish an emergency operations center (EOC). The EOC is a meeting point for you and fellow staff. It is also the site where communication links are centralized and information is distributed to emergency personnel, school employees, and the community. The EOC can be an office or another location that is not damaged and is accessible to all staff.

   Tip: Establish an unpublished phone number to use for outgoing calls when regular phone lines are tied up by incoming calls.

3. Contact all staff members and brief them on the situation (you may need to think beyond email and phone calls, depending on the damage). Identify who is available and who isn't. Then, hold a staff meeting to get everyone on the same page. Assign tasks and a reporting structure. Establish a schedule for recovery team meetings.

   Tip: Group your action items into long-term and short-term priorities. The list of tasks may seem overwhelming, but organization will help keep moral high. (See the article on page 8 for more tips.)

4. Establish communication links. Contact your utility and telecommunications providers and work to reestablish service.

   Tip: If reconnection is delayed, consider alternative modes of communication (TV, radio, flyers, etc.). The district's staff, teachers, students, and parents will want to know what is happening, so keep communicating.

5. Contact FEMA and the district's insurance company. FEMA has stringent rules for requesting

emergency aid. Likewise, your insurance company will have prescribed steps for receiving compensation for damage. You must be aware of these rules and follow them closely to ensure the district receives compensation and support.

Tip: Go to FEMA's Public Assistance Grant Program at www.fema.gov/government/grant/pa/index.shtm

6. Take inventory. Before you begin cleanup, identify what has been destroyed, is damaged, or is missing. It is absolutely imperative to photograph everything! While you generate photo documentation, create a log with each picture's description. In addition, track all purchases made during recovery, such as tarps, tape, and replacement equipment.

   Tip: Document everything—desks, computers, servers, wiring, power strips, books, and so forth.

7. Contact critical technology vendors. You will need technology supplies and know-how to get your network back online. Identify your critical needs and reestablish those first. Once you are up and running, you can then begin to rebuild the entire network.

   Tip: Don't forget to contact software vendors. Records of licenses may have been lost, and vendors will help identify what can be replaced legally.

8. Reestablish payroll quickly. Your community may have come to a halt due to this crisis, but the rest of the world is still operating.

   Tip: You and your staff need money to survive, so make payroll the top priority.

9. Recover data. The data contained on your old servers are invaluable. Although the information may be lost, it is oftentimes recoverable. Many companies offer services to capture critical data from damaged servers.

   Tip: If your data are backed up off-site, alert your provider to the situation.

10. Begin the cleanup process!

No district wants to deal with a crisis or disaster of any type, but addressing the potential tragedy before experiencing it is critical. Detailed planning, redundancy in personnel and equipment, and drills and practices for preparation and response are the keys to ensuring that you can quickly and efficiently restore mission-critical operations and focus on the business of learning.

CoSN has resources available to support you in you the planning process at www.cosn.org/itcrisisprep and www.cosn.org/cybersecurity

Linda Sharp is project director of CoSN's IT Crisis Preparedness Initiative. Email: lsharp@cosn.org