Crisis Preparedness: Leadership for IT Disaster Recovery

Backgrounder Brief

Disaster recovery planning for a district's IT systems and resources must be a priority focused on expecting and being fully prepared for the unexpected.

Disasters have become all too familiar in America in the last several years. Media attention most often focuses on the impact of the disaster and initial response efforts. In the background, when response efforts are most successful and recovery operations most immediate, there has been careful and comprehensive preparation and planning.

Your schools are perhaps running 24/7. When there is the unexpected disaster of any kind, school personnel, students, parents and communities expect to rely on communication and critical services such as payroll and access to student information the district provides and therefore the technology that supports them.

Disaster recovery of IT-related operations and information is critical to the 24/7 operations of your district and its overall business continuity planning. Communication and the continued availability of services are critical for school stakeholders. This strong reliance on technology presents significant challenges to today's school technology leader.

Leadership is required to make disaster recovery planning a priority.

Defining Disaster Recovery

Disaster recovery is the ability of an organization to resume its operations after a disaster.

IT disaster recovery, one component of overall business continuity planning, refers broadly to precautions and coordinated steps that help identify and analyze risks, minimize the impact of the disaster and then enable the recovery of business and IT systems following the disruption.

A disaster recovery plan includes a subset of tasks, resources and functions such as identifying vital records and other critical information, determining and prioritizing recovery needs and having backup solutions for data, equipment and people resources.

CoSN
ESSENTIAL
LEADERSHIP
SKILLS SERIES

Consortium for School Networking • 1710 Rhode Island Avenue NW, Suite 900 • Washington, DC 20036-3007
(p) (202) 861-2676 (f) (202) 861-0888 (w) www.cosn.org (e) info@cosn.org

CoSN—Your Voice in the Future of Education Technology

Sub-plans focus on what happens before, during and following a disaster:

1. **Mitigation and prevention**
2. **Preparedness**
3. **Response**
4. **Recovery**

Considering Potential Disasters and Performing a Risk Assessment

Disaster recovery plans need to address the broad range of potential disasters—natural disasters, man-made crises, digital threats, medical emergencies and others. The first step in this planning effort is to perform a risk assessment or risk analysis to consider all possible threats and vulnerabilities and the consequences of each.

A risk assessment involves stringent analysis of the processes and functions of your district deemed most critical. As part of the assessment, you identify the range of types of disasters that could occur and then determine what the impact would be if your technology-supported systems failed. Prioritize based on what, for your district, would be an acceptable period of unavailability of each service or operation. This alone is a tremendous exercise when taken down to the level of all of the minor implications of a failure of service.

You cannot really begin the development of your disaster recovery plan without first going through this questioning exercise and gathering input from all stakeholders to identify and classify services, operations and records. Conducting the risk analysis provides the foundation for your IT disaster recovery plan.

Developing Your Disaster Recovery Plan

Your plan should be easy to understand and easy to follow. It should be organized into sections that address specific kinds of disasters and outline each task to be accomplished. It should provide for redundancies—backups—in people and resources. And it should have general information that can be efficiently communicated to all stakeholders and then clear, specific, detailed sets of tasks for those responsible for specific disaster recovery activities.

The first priority is ensuring the safety of students and staff. Your other objectives include protecting enterprise resources: ensuring the safety of files and vital records, ensuring the safety of equipment and facilities and maintaining communication and productivity.

Imagine that tomorrow your district's IT team is faced with a disaster. Scale your plan to the unimaginable, worst-case scenario. Imagine that they have no access to their offices or school buildings. Imagine that they have no access to any of the district computers or other technology. Imagine that all phone lines are down and cell towers out. What resources would be lost, what data would be critical, how would you communicate with staff and the community and how would you begin to restore communications, operations and a sense of community?

Your disaster recovery plan will provide the roadmap of what will be done, by whom and how.

Identifying Resources Needed and Planning Processes

Effective disaster recovery planning must reach broader than the technology-supported systems and infrastructure.

You have relationships with a range of technology providers, some of whom will be central to your IT disaster recovery plan. Identify each one critical to your plan and evaluate their own emergency response preparedness and ability to respond to your needs in the timeframe you would require in a disaster.

In a disaster, you will need to be able to smoothly and quickly work with and coordinate with other local, regional, state and federal agencies and authorities and their teams. Community-wide partnerships are critical to the success of your plan. Your shared goal is a coordinated plan of response.

Communicating the Plan

Communication is an essential component of your disaster recovery plan. It is your people, not your technology, which will ultimately ensure that your plan works. In the event of a disaster, your plan can help ensure student and staff safety, ensure communication and critical operations and move your district to an efficient and timely recovery.

Create individual reference guides with function-specific response and recovery checklists and key information for each assigned role in the plan. The disaster recovery plan should be a physical document and not available online only.

Remember too to provide copies of the written plan to key partners, providers, consultants and emergency preparedness agencies with whom your district works.

Practicing and Testing the Plan

The time to test out your plan is not when your district is facing a disaster. Don't just create the plan—communicate it and then practice it. Like communication, training and testing are essential components of your IT disaster recovery plan. One of the best ongoing communication vehicles is to practice the plan.

Build in periodic review of the plan and be certain a process is followed such that new applications and data systems and revisions to them are integrated with an eye to disaster recovery needs and appropriate plans for recoverability. You want to be certain your disaster recovery plan is always current.

Ensuring Redundancies

When the experts on disaster recovery and business continuity discuss best practices, the word you hear repeated over and over again is "redundancy". Be sure you have redundancy at every level of equipment, services, data and people.

Developing a sound IT disaster recovery plan for your district will necessitate a significant investment of time. Communicating, revisiting, reviewing and periodically testing and troubleshooting the plan are all necessary to ensuring you have a successful plan should you need it.

Lives may well depend on the execution of a sound plan in the event of a disaster. When did you last review your district's IT disaster recovery plan?

This Backgrounder Brief is an executive summary of *Crisis Preparedness: Leadership for IT Disaster Recovery*, a component of CoSN's Essential Leadership Skills series. CoSN, a national non-profit organization, is the country's premier voice in education technology leadership. CoSN's mission is to serve as the national organization for K-12 technology leaders who use technology strategically to ultimately improve teaching and learning. CoSN provides products and services to support and nurture leadership development, advocacy, coalition building, and awareness of emerging technologies.

For more information about CoSN, including information on how to join, see www.cosn.org. For more information about the CoSN Essential Leadership Skills series or to purchase components, see www.cosn.org/catalog/.

Published: 2006