

The Optimal Reference Guide:

Disaster Prevention and Recovery for School System Technology

Extraordinary insight into today's education topics

Glynn D. Ligon, Ph.D., ESP Solutions Group
Evangelina Mangino, Ph.D., ESP Solutions Group



ESP Solutions Group

When a hurricane, flood, fire, or earthquake hits, what really is the disaster for a school system? The weather event is really a cause. The disaster is the effect of that cause. When a student has to change schools, records may be lost or so long in arriving at the new school that services are delayed, assessments must be re-administered, or class assignments must be changed. Then the real disaster is the student's lost learning opportunities. This simple change in perspective allows us to approach disaster recovery such that educational services to students are the top priority for continuation or recovery, not the physical aspects of technology.



“Are our own student data secure? If fire, flood, earthquake, or plague of locusts were to destroy our workplace, would our records and working files still be accessible?” --Peter Hendrickson, Ph.D., President of the National Association of Test Directors

Insights

As ESP Solutions Group researched best practices for disaster recovery, we had several key insights.

1. Published disaster recovery planning processes are grounded in business technology architectures, not school system realities.
2. Disaster recovery planning focuses more on replacing or backing up the pieces of technology than a comprehensive plan to continue access to the information and software applications upon which educators depend.
3. The commercial and governmental guides, which are available to help information technology professionals, leave too much of the design and work up to the local staff, rather than provide practical, school-system-grounded documents and templates to complete.
4. None of the guides provide the project management support structure required for a successful planning process.
5. Existing school system disaster recovery plans reflect so much of their priorities, software products, technology standards, physical facilities, and people that they provide only general patterns for another school system to review.

The reality is that we did not find an acceptable published guide for our school district clients. So we have described in this white paper a two-phase process to guide a school system through the steps required for a solid disaster prevention and recovery plan.



Disastrous Conventional Wisdom

What some people would accept as conventional wisdom may actually lead to disaster. Attitudes such as “It won’t happen here.” and “I don’t have the time or resources to develop a plan now.” are obvious unwise perspectives. Thinking that disaster prevention and recovery are covered by security plans is another. Here are some myths associated with disaster recovery and their realities.

MYTH: Events such as hurricanes, earthquakes, fires, and floods are disasters for school systems.

REALITY: In fact, the effect of the event is the real disaster. Knowing this is crucial in the planning and preparation process, because the effect should be the focus of a disaster plan. If the recovery plan does not revolve around the educational processes that a school system must provide, then a seemingly successful restoring of technology may not result in a resumption of the learning process for students.

MYTH: The most common cause of a school system’s technology disaster is weather, earthquake, flood, or fire.

REALITY: Loss of electrical power is the most frequent cause of a disaster.

MYTH: Disaster recovery is the same in school systems as it is in other organizations.

REALITY: Disaster recovery is not the same in a school system as it is in other organizations. School systems have more crucial software applications, distributed systems across many campuses, site-based decisions about technology systems, and a public interest in the outcome.

MYTH: A comprehensive disaster recovery plan takes a long time to put in place.

REALITY: Actually, most plans do take a long time (over a year) to establish. However, the planning and preparation process should be completed within about six months to ensure availability and consistency throughout.

MYTH: Most disaster recovery plans are comprehensive enough to ensure continuation of an organization’s important processes.

REALITY: Most disaster recovery plans are not comprehensive enough to ensure continuation of an organization’s important processes. School system plans typically cover their central information

 **ESP Insight**
The challenges faced by schools in the event of a disaster are highly differentiated from challenges within other organizations.

technology center. In school systems, there are extensive hardware installations and software implementations at school sites outside the central facilities. These are typically not covered directly by an IT department's plan.



In school systems, there are extensive hardware installations and software implementations at school sites outside the central facilities. These are typically not covered directly by an IT department's plan.

MYTH: Disaster recovery plans should focus on replacing hardware, networks and software installations.


REALITY: A successful disaster recovery plan will focus on managing people to do the right things before and after a disaster.

MYTH: Back-up data files are adequate for a full recovery of most software applications.

REALITY: Back-up data files are not adequate for a full recovery of most software applications. A typical back-up file is a limited, encrypted data set that merely replaces a lost file. For full recovery, a school system needs configurations and detailed set-up documentation. A back-up file is also not in a format that can be shared with other applications or read successfully in the event the data must be imported into another application.

Best Practices for School Systems

ESP's research identified several principles of best practices that apply particularly well to school systems.

 **ESP Insight**
Priorities for recovering specific educational systems can change depending on the timing of the event.

1. The timing of an event determines the priority for recovery of the technology that supports basic processes. For example, an event occurring early in a grading period may require the priority for disaster recovery to be on payroll or instructional management rather than report card production.
2. Prevention is better than recovery. Putting in place effective damage mitigating measures can ensure the continuation of processes rather than the recovery of processes.
3. Project management processes are required for successful plan development. Creating and implementing an effective disaster prevention and recovery plan requires the scheduling, coordination, communication, and management of complex activities and groups of stakeholders.

 **ESP Insight**
The involvement of all stakeholders is the key to a comprehensive, successful recovery plan.

4. The involvement of all stakeholders, not just IT staff, is necessary. IT staff know the technology hardware, software, and network intricacies, but the educators know what needs to be done with and for students the day after an event.
5. Each software application must be included in the plan. School systems may have three dozen or more software applications that need to be restored after an event. Each one will have idiosyncrasies that must be accommodated, e.g., separate servers with unique configurations, contrasting data back-up processes, and different people who know what to do. ESP Solutions Group has identified 43 information-based functions that are typically supported by software applications.
6. Applications and services hosted off-site and/or by vendors must also have a plan. Seldom do school systems require a vendor to demonstrate recovery capabilities as a requirement before signing a contract. Requests for bids/proposals should require vendors to provide a disaster recovery process that is compliant with the school system's plan.
7. School systems have many pieces of information that are collected and kept on paper only. Because paper records can be impossible to recover in some situations (fire, flood, misplacement of boxes, etc.) a school system should move paper documents to electronic media as soon as possible.

To ensure comprehensiveness, to avoid the pitfalls of conventional wisdom, and to follow best practices, a school system must implement a carefully managed planning process. ESP Solutions Group's certified project managers joined with our technical experts to describe how a school system should create a successful disaster prevention and recovery plan. The key steps are:

Phase I: Needs Assessment and Buy-In

- Complete a study to identify priorities and needs. This needs assessment should identify the processes and applications that must be recovered, and the recovery provisions currently in place. The study results will justify the resources and priority that will be needed.
- Assess buy-in by policy and administrative leaders. Because the disaster prevention and recovery plan goes far beyond the IT department's doors, all stakeholders across the school system must be involved — and support the plan.
- Review adopted policies. Guidance and authorization from the highest level are necessary for the plan to receive adequate funding and support.



For an effort like this to succeed and reach full implementation in a school system, you must have the following:

- *Buy-in by key stakeholders*
- *Confidence that the efforts will be completed successfully*
- *Resources to match the requirements*
- *Project management skills to succeed in a school system full of competing priorities*

Phase II: Design and Implementation

- Develop a project charter and project management plan for the planning process. The best project management practices will be necessary to develop and implement a plan within a reasonable timeframe.
- If the current school system policy is not supportive of Phase I and II, listed here or if a disaster prevention and recovery policy does not exist in the school system, a policy must be written and adopted.
- Identify the school system's basic processes, functions, and applications. This is where a disaster prevention and recovery plan for a school system becomes differentiated from those in other organizations. Dozens of processes and software applications are employed by schools to carry out their functions from instructional management to building security.
- Develop and implement the disaster prevention and recovery plan. Each component of the plan must be specified in detail, and then implemented.
- Test the plan. **Warning: Some disasters are the result of a failed disaster recovery test.** Periodic testing of separate components and the overall plan is required to ensure that the plan itself is up-to-date and functional.
- Maintain the plan. Changes and new components will be occurring continually. Each will require a review of the plan.
- Evaluate the success of the plan after an event occurs. If and when an event occurs, a thorough evaluation of how well the plan functioned will be needed. The evaluation process should be a part of the plan itself.

Access to Student Records After a Disaster

If students move to another school system after a disaster, how do their official school records follow them? That contingency must receive significant attention in the disaster prevention and recovery planning process.

One alternative is to create a “vault” containing the most recent student records for every student. The vault would be accessible by an authorized receiving school if the sending school’s records are inaccessible.



Mirroring student records in a “vault” provides timely access when an event occurs.

The National Transcript Center (www.transcriptcenter.com) offers a WebDAV solution that mirrors a student’s data within the school’s student information system for access whenever a transcript is to be sent. This staging area serves as a ready source of official student records in the event that the school’s student information system is unavailable. Thus, students who show up at a new school can have their records requested and electronically delivered quickly.

**“If our students are scattered to the winds, would their records be clearly understood by a receiving district?” --
Peter Hendrickson, Ph.D., President of the National
Association of Test Directors**

Disaster prevention and recovery planning is like many discretionary activities in a school system. A champion or several are typically needed to ensure success in the face of so many competing priorities. In this arena, the champions can come from IT, instruction, the board of trustees, administrative leadership, the community, or campus management. Whatever the organizational status of the champions, reality demands that disaster prevention and recovery be a team effort across all the schools, departments, and programs.

What to do next:

If you would like more information on ESP's Disaster Prevention and Recovery products and services, such as a needs assessment or designing a comprehensive plan, please contact us by email at nodisaster@espsg.com.

Key Terms

Application: A computer program used to accomplish specific processes not related to the computer itself. In a school system, core applications include the student information system, finance, human resources, instructional management, food services, media services, health services, transportation, and special program management.

Backup: Backup refers to the process of copying information from disk to a secure storage medium (usually tape), and backup also refers to the storage medium itself.

Best Practice: A combination of what school systems are doing successfully and what they believe to be even better practices that they would follow if they could.

Business Continuity Planning: Business continuity planning (BCP) is a procedure put in place by an organization to ensure that essential business processes continue following a disaster. The BCP takes into account the need for alternate facilities (offices, warehouses, and retail outlets) if normal business locations become inaccessible. A host of other items are included in the plan, including departmental guidelines detailing how to maintain business operations under extraordinary circumstances.

Disaster Recovery Planning: Disaster Recovery Planning (DRP) is a subset of Business Continuity Plan and focuses solely on the recovery of IT systems. The DR plan, the output of the DRP process, documents procedures for IT staff to follow when reestablishing business system functionality after an outage. Each business application must be cataloged, its recovery needs assessed and documented, and the importance of the application to the organization quantified to enable IT staff to prioritize the recovery process. Symantec, 2003

Disaster: The negative effect of not having access to information. Some examples are: denial of services to a student who is moved after an event occurs, payroll checks not being issued on time, incorrect district or school accountability ratings.

Disaster Prevention and Recovery (DPR) Plan: A written process with proactive steps to help prevent a core application outage; a plan for processing core applications in the event of a major hardware or software failure, or destruction of facilities.

Event: The cause of a temporary or permanent disruption to access to information. Some examples are: power failure, human error, hurricane, fire, and earthquake.

Function: A process followed by people within a school system to access information and perform their work.

Information Technology (IT): Usually a separate department within the school system that is responsible for the implementation and support of hardware, software, and network infrastructure and services.

Prevention: Proactive steps taken to avoid the disruption of access to information.

Preventive Controls: Checks and balances put in place to be proactive to prevent an action, in this case a disaster.

Risk Management: The ongoing process of assessing the risk to school systems as part of a risk-based approach used to determine adequate security for an information system by analyzing the threats and vulnerabilities and selecting appropriate, cost-effective controls to achieve and maintain an acceptable level of risk.

Vault: A secure location for storing data for use in recovery or for continuation of operations during recovery.

WebDAV: (Distributed Authoring and Versioning) An extension to the Hypertext Transfer Protocol 1.1 (HTTP/1.1) that allows for the manipulation (reading and writing) of objects and attributes on a Web server. Exchange 2000 natively supports WebDAV. Although not specifically designed for the purpose, DAV allows for the control of data using a filing system-like protocol.

References

Contingency Planning Guide for Information Technology Systems. National Institute of Standards and Technology, 2002.

Data Management Strategies for States and Districts: An ESP Whitepaper for Data-Driven Decision Making. Ligon, G., ESP Solutions Group, 2005.

How Data Can Help. Armstrong, J., & Anthes, K., 2001. American School Board Journal 188(11), 38-41.

Katrina, Rita, Children in Poverty, and Test Directors. Hendrickson, P., 2005. National Association of Test Directors Fall Newsletter. Available at www.natd.org.

Plan to Stay in Business. U.S. Department of Homeland Security, 2005. Available at <http://www.ready.gov/business>.

Safeguarding your Technology: Practical Guidelines for Electronic Education Information Security. National Center for Education Statistics, 1998.

Using Data to Improve Schools: What's Working. American Association of School Administrators, 2002. Available at www.aasa.org/cas/UsingDataToImproveSchools.pdf.

Weaving a Secure Web Around Education: A Guide to Technology Standards and Security. National Center for Education Statistics, 2003.



About ESP Solutions Group

ESP Solutions Group provides its clients with *Extraordinary Insight™* into K-12 education data systems and psychometrics. Our team is comprised of industry experts who pioneered the concept of “data driven decision making” and now help optimize the management of our clients’ state and local education agencies.

ESP personnel have advised school districts, all 52 state education agencies, and the U.S. Department of Education on the practice of K-12 school data management. We are regarded as leading experts in understanding the data and technology implications of the **No Child Left Behind Act (NCLB)**, **Education Data Exchange Network (EDEN)**, and the **Schools Interoperability Framework (SIF)**.

Dozens of education agencies have hired ESP to design and build their student record collection systems, federal reporting systems, student identifier systems, data dictionaries, evaluation/assessment programs and data management/analysis systems.

To learn how ESP can give your agency *Extraordinary Insight™* into your K-12 education data, contact Evangelina Mangino toll-free at (888) 828-6480 x123 or emangino@espsg.com.

This document is part of *The Optimal Reference Guide Series*, designed to help education data decision makers analyze, manage, and share data in the 21st Century.

Disaster Prevention and Recovery for School System Technology, Copyright © 2005 by ESP Solutions Group. All rights reserved. No part of this paper shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher.



ESP Solutions Group

(512) 458-8364

www.espsolutionsgroup.com

Austin • Boston • Washington DC