Disaster Recovery Planning For School Districts

Revision Wednesday, July 28, 2010

Central New York Regional Information Center at Onondaga-Cortland-Madison BOCES
Information Security & Disaster Recovery Services
http://CNYRIC.org
315/433.2280

WHAT & WHY

Our customers have asked for guidance in the preparation of their disaster recovery plans. To respond to this need, we have prepared a high-level outline for a disaster recovery plan.

This outline is a modified version of the existing CNYRIC disaster recovery plan and an expansion upon a presentation explaining our recommended plan. Screen captures of that presentation appear throughout this document. This outline is reflective of modifications we are making in our existing plan. They include updates to reflect changes in personnel, facilities, and technology. Other content additions and enhancements reflect changes in communicated expectations from auditors.

Within this outline we have also tried to begin the process of sharing guidance and perspective about best practices in disaster recovery planning and implementation. Revisions will be implemented periodically and we encourage and appreciate any feedback readers of this document might have for us. Any feedback should be directed to Steven J. Tryon, Manager of Information Security & Disaster Recovery for the Central New York Regional Information Center (CNYRIC). Email contact is sjtryon@CNYRIC.org and phone contact is 315/433.2280.

Far more important than auditors, mandates, and guidelines is the safety and security of the students you serve and the employees of your organization. Those issues should be addressed within your organization's safety and security plan(s). This outline focuses only on your information systems and **should simply be one element** of the organization's disaster recovery plan. That plan should reference the plan based on this outline for all matters related to your digital infrastructure and systems. Done correctly, technology does **not** drive disaster recovery planning for your organization. Rather, technology systems are prioritized for recovery along with other organizational systems.

Implemented properly, anyone with reasonable levels of technology systems-related skills[1] will be able to use the plan generated from this outline to recover an information technology system when asked to do so by an incident commander. (Incident Command System)

[1] Obviously, the required technical skills will vary dramatically depending upon the system being restored. Idealistically, your plan will explain each system restoration in the most simplistic manner possible.

The Fine Print

There is no perfect plan nor is there a perfect plan outline. Every school district is different and has its own set of issues to address; geographic, financial, technical, political, etc. Therefore, the CNYRIC does not warrant the suitability of this outline for any specific disaster recovery plan or process and you will have sole responsibility for determining the suitability of this outline for your situation.

Our objective with this outline is to help you get started on a plan. When you are ready to write and/or implement your plan, we offer a collection of services that will help you complete the project. Our services include plan development (everything from researching the structure of your organization to the actual writing of the document), testing of the plan (from tabletop experiences to actual incident tests), plan promotion (presentations, staff training, organizational awareness), and an array of implementation services (off-site backup, hosting, rack space, office space, and other solutions to assure the critical systems of your organization resume functioning as soon as possible).

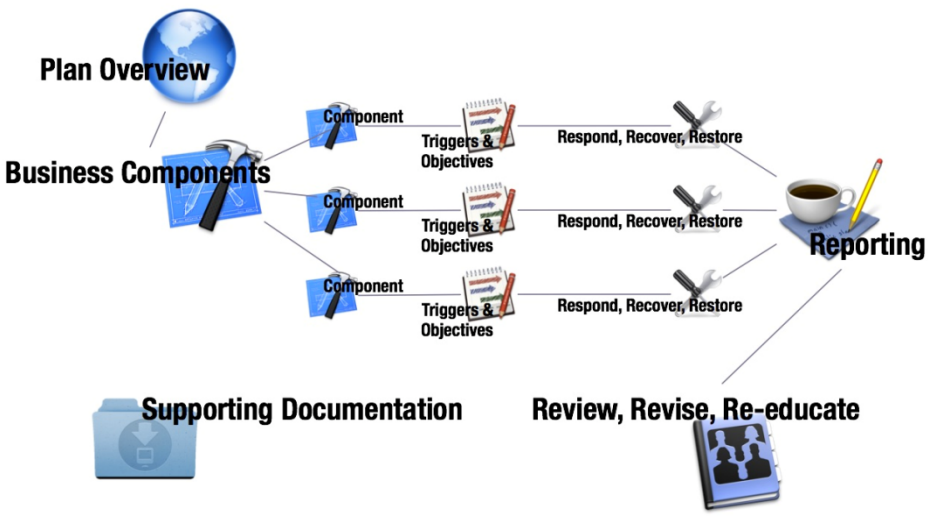
We encourage you to contact us if you have any suggestions or comments about this outline. The issues we face constantly change so your plan (and this outline) should adjust accordingly. And, should you need support completing your plan, we stand ready to assist you.

On behalf of the entire team at the Central New York Regional Information Center, thank you!

Steven J. Tryon
Manager, Information Security & Disaster Recovery

Outline Contents

A final plan should contain at least the following elements:



Plan Overview • *What is the plan all about? What are your intentions & goals?*

Business Components • *What are the pieces of your world?*

Triggers & Objectives • *When will you react & to what extent?*

Respond, Recover, Restore • *What actions will you take?*

Reporting • *What will you document & communicate?*

Review, Revise, Re-educate • *How will you arrange to do it better the next time?*

Supporting Documentation • *What are the materials that make carrying out the plan possible & where are they kept?*

Plan Overview

[What is the plan all about? What are your intentions & goals?]

This introductory section of your plan should fully describe your organization's risks, outlook, and posture relating to disaster recovery. It should demonstrate that there is a coherent and organization-wide understanding of your objectives, the personnel involved in these activities, your priorities for response, and explain all of your plan-related training and testing activities. **It is this section of the plan that communicates everything anyone should need to know before any disaster situations. The sections of the plan following this overview are those that are relevant during a disaster situation.**

BUY-IN

Your organization must be supportive of this plan if it has any hope of being successful. This success begins by obtaining plan support from your district office (the Superintendent and perhaps even the Board of Education). Often, it may be helpful to include a letter from this level of your organization within the plan that conveys those assurances. The success of the plan is then solidified by assuring that all levels of the organization are aware of the plan, know their role if the plan is executed, and have agreed to abide by the instructions it contains.

Integral to professed support of the plan are assurances that funding will be available to support details of the plan. This must include funds to obtain any needed resources and to continue support for all the resources that are put into place. Budgets change every year so regular review of the plan needs to be part of your budgeting process. This may also require annual reminders to key personnel about their commitment to the plan and of the importance of the plan to the organization in a time of crisis.

TEAM

When an incident occurs, there are sure to be several roles that will be involved in carrying out this plan. Describe these roles using the job titles used within your organization to aid in the longevity of your written document, minimizing the need to update the plan whenever there are personnel changes. Make sure that the people filling these roles know their responsibilities and are properly trained to carry them out. Be attentive to any personnel changes within your organization that impact the plan and adjust accordingly with communication and training (these activities are described more fully in the section of this document about education).

The roles include:

- ***INCIDENT COMMANDER***. *During any scenario, the Incident Commander is responsible for overseeing all activities of the response. It is from this role that direction is provided regarding how a response will be conducted. This role should already be identified in your organization's incident response documentation. (Incident Command Structure For Schools)*
- ***TECHNOLOGY DIRECTOR***. *This role is responsible for taking direction from the Incident Commander and supervising the technology-related responses according to the priorities of the plan. This role will also be responsible for communication between the Incident Commander and the technology response personnel. This role will also include any required technology-related vendor/partner management.*
- ***SYSTEM ADMINISTRATOR***. *This role will be responsible for the protection or restoration of technology-related systems. They will also be required to keep the Technology Director informed of response progress and providing the documentation of all activities conducted during the response.*

It is also important to understand that in an incident, the command structure may be led by someone outside of your organization; a fire chief, peace officer, or other emergency services role. Your ability to provide them with your plan and know your role and responsibilities will aid in a much more efficient response to the incident.

Business Objectives

During a response there should be no need to make decisions about which systems receive your attention. It is important to understand that during an incident, the mission of the organization may temporarily change so no assumptions should be made regarding system restoration. In an incident involving a geographic region, the organization may be required to focus on supporting community needs rather than internal needs. The organization, in its full incident response plan, should identify the systems to receive your attention in the order in which they are to be placed back into service. Safety and security of students and personnel will assuredly be the priority over financials, student data, etc.

Whether identified in the larger plan or not, this section of the plan should list all technology-based systems and their priorities for restoration. With that prioritization, fully describe the level of restoration necessary and the timeline for that restoration. For example, a financial system may be your first priority, but it may be necessary to assure that modules related to purchasing are functioning within hours while accounts payable be back on-line within some number of weeks. In between, the priorities may identify email (or other) systems that must be restored within days. Map out/diagram and clearly identify this timeline for all of your systems.

Risk Analysis

Your plan should identify all of the risks that you believe could jeopardize your systems in some way. Working through this process will help you to make decisions about the types of responses you may need to take as well as the support you will require during those responses.

Most organizations might identify fire as the largest risk they face. This list might also include attacks related to viruses, bots, or any of the other evolving threats to our digital systems. And don't overlook some of the larger threats you might face. During the time during which this document was initially prepared, our region experienced at least two confirmed tornado strikes and one earthquake! Other parts of our region are within flood plains and must consider a response to that type of scenario. Some regions include nuclear power facilities that require their own unique types of incident responses.

Completing this section of the plan will also help you to identify the risks for which you have no capacity for response. Discovering these risks will help you adjust your technology planning to mitigate their potential impact.

Consider any possible cascading risks that might be encountered. For example, threats to a database server system would also impact the systems dependent upon the information it contains. Risks that you relate to that system may be those that you rank higher in your list to prepare for.

Assumptions

Use this section of the plan to help identify weaknesses and restrictions that keep you from having a *perfect* plan. Hopefully, your on-going work will see the items in this area reduced or eliminated.

Within the planning process, you may discover boundaries. For example, if your organization is without a comprehensive incident response plan you may not be able to identify the Incident Commander for your organization. You might also uncover resistance by organization leadership to establish response priorities. Regardless, document those boundaries as well as any mitigation you will take (like seeking an organization incident response plan or helping district administration to come to conclusions about system priorities).

Also critical to this section of the plan are the boundaries that you discover to exist for any plan actions. As an example, your district might be rural enough that reconnecting to a WAN or the Internet in an incident are completely outside of your control and completely dependent upon others. Knowing and documenting these issues will save you incredible frustration in an incident when your customers are all looking at you to provide a service that just cannot be provided. Placement of these issues within this area of the plan makes sure that your district is aware of these problems in advance. This should also provide you with a list of action/budget items that you can work toward correcting. It also may simply be that your organization, while recognizing the risk, chooses not to take any steps toward mitigation. Most importantly, the risks are identified and communicated through this section of your plan.

STRATEGY

The strategy section of your plan helps to add some perspective to your response as well as identifying some variations that may impact a response.

For example, as a school district your strategy for response may be somewhat different during summer months when students are not in your facilities. Or perhaps you have special summer activities that use facilities in different ways that force a variation of the plan. Identify and describe any of these things within this area of your plan.

It is recommended that you have as few variations as possible! The best solution is to have a solid plan, on which district personnel are trained, and that is implemented the same way every time. That is the least confusing for those involved in a response as well as those impacted by a response.

EDUCATION

This plan will be completely useless unless the people carrying it out are fully educated to its purpose and their role within any response. Within this section of the plan, several things should be documented and subsequently implemented.

Primarily, the individuals (serving in the roles) specifically identified in this plan must know the contents of the plan and the actions they are to take. An initial training and regular refresher training must be created and documented here. Important to this process is a plan to provide that training whenever there are personnel changes impacting the identified roles. People change jobs and titles may be created or lost. With each of those changes, new training and possible plan adjustments must take place.

Beyond those identified roles, the rest of your organization must be educated to the contents of the plan. While they may not play a specifically identified part in any responses, they need to know what to expect during those times. This reduces confusion and establishing expectations should minimize the time spent answering their questions while you and your team are involved in a response.

Training for plan participants is probably best suited in the form of the tabletop testing (described in the Testing section of this document) with periodic refresher activities conducted in the form of mandated on-line tutorials (or similar). For the rest of your organization, on-line training, newsletter-style communication, posters (or similar) may be sufficient to set their expectations and identify how they should react.

Testing

No assumptions should be made regarding the suitability of your plan. You must test it in order to work out any issues. The testing process can also be used as your way of educating those serving a role in the plan. Within this section of your plan, document your testing processes, those involved and responsible for making them happen, and the frequency with which they are conducted.

Tabletop tests are probably the best way to conduct this process. To implement these, all of those involved in the plan should be gathered together. This will be an excellent opportunity to bring about awareness to the importance of working through incidents as a team and in advance of any real situations. Those gathered should include anyone involved in the organization's incident response, not just those directly related to technology. Representation should include the district office, business office, facilities (buildings and grounds), pupil services, human resources, etc.

These experiences are best conducted by talking through an incident based on one of the risks identified earlier in this plan. This process will demonstrate the interrelationship among the represented groups and their dependency upon each other in an incident. Participants will be thinking about their own areas of responsibility as they hear what others would be doing during an incident. By putting these thoughts in context with the probable action of others, the proposed plan can be refined to best meet your stated objectives.

Most school districts will also need to include vendors of products and services within the testing process. In most cases this will simply be to contact current providers to determine their ability to deliver those services in short notice or during some sort of regional crisis. The list of service providers you contact should also include your designated BOCES and your Regional Information Center. Ask lots of questions about how they are prepared to address the risks you identified in your own plan. You may also need to contact new vendors who would provide services you might need only in case your plan is activated. Make sure that they too are prepared to deliver what you need during a time of crisis.

Finally, there are collections of other tests that you should conduct to assure your plan is the best it can be. Those include technical tests like verifying your backups, checking on the status of battery backup systems, powering-up any cold/warm sites you have in place for mitigating incidents, testing alternative communication tools (phones, two-way radios), etc. Within this section of the plan, document all of these activities. List all of the testing you conduct and the frequency with which it takes place.

Plan Activation

The next section of the plan serves as a reference tool and instruction manual if the plan is ever called into action.

Business Components

[What are the pieces of your world?]

Within this section, every technology-based system/solution used by your district should be identified and described. Descriptions should include what the system does, who uses it, its software and hardware requirements, configuration settings, access permission structures, contact details for the individual primarily responsible for the system as well as any associated vendor/manufacturer, etc. A form that can be used to work through the collection of all these details can be found on our web site.

It is crucial that this section of your plan be organized according to the results of a business impact analysis that should be conducted by your organization. That analysis should determine which technology (and other) systems are critical (urgent, perhaps mandated by law) and those that are non-critical (not urgent). Each system in the organization should be assigned a specific priority and in the event the plan is called into action, system protection/restoration activities should **only** be conducted in the sequence determined by these priorities. Depending upon the available resources, activities might be conducted in parallel during this process to conclude them more quickly, but the priorities should **never** be disregarded. Adhering to these priorities eliminates confusion, sets the system restoration expectations for all users of these systems, and assures that restoration activities are aligned with the larger organization goals.

TRIGGERS & OBJECTIVES

[When will you react & to what extent?]

The description of each business component should also include guidelines regarding likely scenarios for response. For example, the restoration process for a system destroyed by a disaster will be very different than the response that might be triggered by the threat of a disaster. These different responses need to be described and should be based on the risks that have been identified earlier in your plan.

For each of these types of response, identify the recovery point objective (RPO; how much system functioning/capacity will be restored) and the recovery time objective (RTO; when will that measure of functioning/capacity be restored). These details will also help district personnel to know what to expect regarding when systems will return to a functioning state and what that state will allow them to accomplish in their work.

Respond, Recover, Restore

[What actions will you take?]

For each business system, instructions will need to be provided to bring the system to the state identified by the recovery point objective(s). These instructions should be written in a way that would allow them to be carried out by someone with technical expertise, but without familiarity with the system. Clearly, developing these instructions can be a complicated process. There is also the possibility that simplified instructions are not feasible. Regardless, it would be unwise to assume that the individual(s) currently responsible for the system will be available during a disaster situation. These steps may need to be conducted by someone else on your team, someone from your BOCES or RIC, or perhaps even a vendor. Whomever is assigned the task will need to know the recovery point objective, the recovery time objective, the details relating to reestablishing the system, and all of the configuration details needed to reload backup data, security settings, etc.

REPORTING

[What will you document & communicate?]

The work that is conducted to bring systems back on-line must be documented. The disaster situation is likely to put considerable pressure on all available resources, but that pressure and the (probable) chaos of the disaster make this documentation even more critical. Reviewing this documentation may be the only way to determine why a restored system isn't performing as expected.

Beyond this documentation, status information must be communicated to the incident response team. They will need to know if recovery point objectives and recovery time objectives are being met so that they may communicate those details to district personnel and others involved in and impacted by the recovery efforts. If objectives aren't being (or going to be) met, your reporting will also help the incident response team to determine the need for additional resources.

Please be aware that some of this communication might be included in the organization's crisis communication plan. Defer to anything contained in that plan and make sure this plan aligns with it.

Review, Revise, Re-educate

[How will you arrange to do it better the next time? Post-project reviews / Post-mortem]

This section of the plan describes activities that would be conducted following any incident in which the plan was used. The activities described here should also be conducted following any incidents that did not involve technology systems.

Your plan should describe how, following an incident, the plan will be reviewed and modified. These activities should be conducted with all participants from the incident response team. The objective is to see how people worked cooperatively – toward business continuity goals and how they didn't or couldn't. Those observations should cultivate discussion with the team and ultimately result in modifications to the plan to be better prepared and able to response should there be further incidents.
Any changes that are made in the plan should, if applicable, be shared across the organization to again reestablish expectations during an incident. Using the recent incident as an example in this communication will serve to build confidence from your customers. Make sure that these revisions are also reflected in the training materials you use for your district personnel (for new employees and all refresher training materials).

SUPPORTING DOCUMENTATION

[What are the materials that make carrying out the plan possible and where are they kept?]

Attached to the plan should be all of the supporting documentation that demonstrates and supports the contents of your plan and that would be needed in an incident. In all likelihood, this information is currently scattered across your organization. It is recommended that you implement a way to aggregate the content and provide an off-site backup for time of crisis. This information, along with the plan, should be reviewed periodically to assure its accuracy.

Some suggested documentation includes:

- Names & contact information for the incident response team participants;
- Emergency responder contact information;
- District key personnel & their contact information;
- Vendor contact information;
- Utility contact information;
- Current technology inventory (hardware & software);
- Network diagrams;
- Facility maps;
- Secondary site maps, directions, & access information;
- Secondary site key contact information;
- Technology policies, procedures, & guidelines;
- System configuration documentation & files;
- System documentation;
- System change logs;
- Password locker/storage location & access information;
- Related organization plans (business continuity, business recovery, continuity of operations, crisis communication, occupant emergency, etc).

Every district is different so consider adding any material that will be needed to carry out your plan in the most extreme circumstances. In considering this collection of materials, make no assumptions about who will be available to carry out your plan or what resources will be available at that time. Your documentation should support a response that is conducted at a different location by people who may not even be district personnel.

Additional Support & Recommendations

The staff of the Central New York Regional Information Center at Onondaga-Cortland-Madison BOCES is available to provide a collection of services in support of your disaster recovery planning and implementation. These services assist in the areas of developing your plan and then implementation of the plan:

Plan Development

- Project management & guidance;
- Risk assessment;
- Plan authoring;
- Compliance with comptroller recommendations (to the extent known);
- Incident response team coordination;
- Network mapping;
- Facility mapping & photography;
- Plan-related training;
- Tabletop testing;
- Development of plan-related promotions, presentations, & educational materials;
- On-line documentation hosting & emergency delivery;
- Annual plan review.

Plan Implementation

- Primary site hosting;
- Cold, warm, or hot secondary sites for technology;
- Off-site, network-based backup;
- Secondary sites for personnel during an incident;
- Incident review;
- Plan modification (following an incident);
- Post-incident training.