COURT INFORMATION TECHNOLOGY OFFICERS CONSORTIUM

Disaster Recovery Planning for Technology

Technology Experience Bulletin, TEB: 2007-02

Tips for Implementation

1. **Identify and evaluate risks**
2. **Prioritize business functions**
3. **Prioritize technology services**
4. **Define your recovery strategy**
5. **Facilities matter**
6. **Identify alternate sites**
7. **Use redundancy and fail-over**
8. **Document your recovery plan**
9. **Test your recovery plan**
10. **Keep your recovery plan current**

Disaster Recovery Planning for Technology

It has been said that disaster recovery planning is similar to funeral planning. No-one likes to think about it, and everyone thinks that they still have a lot of time to get it done. The unfortunate reality is that disasters happen. If you are a Court Technology Professional, then disaster recovery planning is an essential part of your responsibilities. This short article will present an outline for developing an effective Disaster Recovery Plan for your organization's technology.

Tip 1: Identify and evaluate risks. The first step in developing an effective Disaster Recovery Plan is to identify and list potentially serious incidents, which could affect normal operations of your organization. This list should include all possible incidents no matter how remote the likelihood of their occurrence. Once you have created this list, rate each incident for degree of probability and potential impact severity level.

Tip 2: Prioritize business processes. Since no technology professional has unlimited resources at his or her disposal, the next step is to determine how you will target your limited resources to provide the most effective disaster recovery provision possible. Work with the functional leaders at your court to prioritize your court's business processes by asking:

Which business processes are the most essential to the court's mission?

What business processes are the most critical to return to operation quickly?

After a disaster, what business processes would not be considered immediately essential in the event of a disaster?

Take recurring process cycles (nightly reports, monthly or year-end processing) into consideration during your evaluation. Disasters often occur at the most inconvenient times.

Tip 3: Prioritize technology services. Once you have an understanding of your court's most critical business processes, you need to map those processes to specific technology components that make those business processes possible. Use this information to identify critical technology environment components, and prioritize each component accordingly.

Evaluate business processes "end to end" during this mapping process. This will help ensure that all technology dependencies are identified and that no false assumptions are made about the availability of ubiquitous

technology in the event of a disaster (E-mail, cell phone service, internet access, etc.). System diagrams and flowcharts can be invaluable tools in this process.

Tip 4: Define your recovery strategy. RTO (Recovery Time Objective) and RPO (Recovery Point Objective) are key concepts to consider when developing a recovery strategy. RTO refers to the amount of time acceptable for returning services or information availability to an organization after a disaster occurs. RPO refers to the amount of data that is acceptable for an organization to lose in the event of a disaster.

Establish RTO and RPO factors for each of the information systems at your court, and in turn assign those factors to the relevant components of your technology environment. For example, if your court can operate without E-mail services for up to 24 hours without severe negative impact, then you might establish a 24-hour RTO for court E-mail services. You would then identify all technical components that your E-mail services are dependent upon (servers, network equipment, internet services, etc.), and evaluate those components in light of your established RTO. Likewise, if your court can lose no more than 24 hours of financial data without severe negative impact, then you might assign an RPO of 24 hours to court financial data. You would then need to identify all of the technical components necessary to provide access to your financial data (servers, software, data restoration systems, etc.), and evaluate those components against your established RPO.

Applying the concepts of RTO and ROP to each of the critical information systems at your court will give you the information you need to develop a technology recovery provision that truly reflects the priorities of your organization. These two key metrics will also be your tools to verify the success of chosen strategies when you test your Disaster Recovery Plan.

Tip 5: Facilities matter. A little careful attention to your technology facilities can pay off big in the event of a disaster. Ensure that the facilities housing your technology resources are constructed and located so that they are secure, protected from extreme environmental changes, and accessible when electrical power is lost.

Remember that relatively inexpensive facility tools can help you avoid some disaster situations altogether: electrical surge protection and power conditioning units, temperature sensors, moisture sensors, seismic bracing, fire suppression systems, and emergency lighting devices, just to name a few.

Tip 6: Identify alternate sites. Having an alternate site for temporarily relocating systems and people can be essential to an effective disaster recovery plan. If you choose to setup an alternate site, keep in mind that your goal should be to establish an alternate location that would still be intact and functioning if your primary location was wiped-out. Use your risk evaluations (from Tip 1) to determine what types of disaster incidents are most likely to affect your primary location, and try to select an alternate location that is likely to survive such incidents. Some important technical considerations for an alternate site include: network services and connections; critical hardware and software; accessibility in the event of a disaster; and resources and knowledge needed to setup and operate your alternate technical environment.

Make sure that you have accurate and current technology environment documentation available from your alternate site in the event you lose your primary (e.g., network topology, equipment configurations, inventory information, etc.).

Tip 7: Use redundancy and fail-over. Today there is a wide range of technology solutions available for maintaining application and data continuity in the event of a disaster. Combining these technologies with a strategy of geographically dispersed technology resources can be a very effective way to protect against data loss.

If you are facing situations with RTOs and RPOs that are measured in mere seconds or minutes, consider technology solutions in which data is continuously and redundantly synchronized across distributed server

clusters or through geographically separate mirrored storage. If your needs are in the range of RTOs and RPOs measured in hours or days, consider data mirroring to stand-by servers or electronic tape vaulting (backups.) Generally, the more demanding your RTO and RPO factors, the more you can expect to pay for technology to support your Disaster Recovery Plan.

Tip 8: Document your Plan. Document your Disaster Recovery Plan in sequential milestones that–in the event of a disaster–will move your organization from a disrupted status towards a return to normal operations. The first milestone should document the process that will deal with the immediate aftermath of the disaster. Start with the step-by-step process that will initiate the Disaster Recovery Plan. This section should include a notification procedure that will be used to contact and inform key employees, emergency services, or other specialists who may need to respond in a disaster situation. Your plan should then move logically through resuming the operation of technology services based on your court's business processes priorities (established under Tips 2 and 3.) Ensure that you identify roles and responsibilities for all individuals and describe duties in the plan.

Make sure your plan is accessible to your Disaster Recovery team even if your primary site becomes unavailable. You cannot afford to assume that anything at your primary location will be available to use in the event of a disaster. Keep multiple paper and/or electronic copies of your Disaster Recovery Plan stored off-site from the physical locations covered under your plan. You might consider storing copies of your Disaster Recovery Plan and supporting documentation on one or more portable computers. These portable computers could travel with key court managers that would be required to respond in a disaster situation.

Tip 9: Test your recovery plan. Regularly test and refine your Disaster Recovery Plan. Regular tests should involve a complete Plan hands-on walk-through, with all responsible individuals acting in their assigned roles to recover your technical environment using the same systems, services, and physical locations that would be used in the event of an actual disaster.

One useful testing technique is to set the stage for assessment by developing a test scenario based on a disaster situation, which realistically could occur at your court (based on your findings from Tip 1.) Using a realistic test scenario to simulate the effects of a disaster upon your technical environment will help ensure that you are conducting a relevant test. When testing is completed, record the results, review the results with your team to identify improvement opportunities, and then update your Plan accordingly.

Tip 10: Keep your recovery plan current. For your Disaster Recovery Plan to be effective, it must be kept up-to-date and applicable to current technology and business processes. This means that any changes must be promptly and accurately reflected within your plan. For this to happen, someone must be specifically assigned the responsibility of ensuring that the plan is maintained and updated, and a process must be in place to ensure that all technology or business process changes are communicated to the assigned person.

Other Considerations

In today's technology dependent world, a Disaster Recovery Plan is often an information technology-focused effort designed to restore operability of target systems, applications, or computer services after an emergency. As valuable as this type of planning is, it can only be effective to the degree that it is one part of a broad, organization-wide planning effort addressing all of an organization's critical business needs in the event of a disaster. This broader organizational planning can take several forms. For example:

Business Continuity Planning (BCP)
This typically refers to a plan for sustaining an organization's crucial business functions during and after a disruption.

Business Resumption Planning (BRP) This addresses the restoration of business processes after an emergency, but unlike BCP, it often lacks procedures to ensure continuity of critical processes throughout an emergency or disruption.

Continuity of Operations Planning (COOP) This planning usually focuses on restoring an organization's essential business functions to an alternate site, with the goal of performing those functions from the alternate site for some defined period of time (30 days, for example,) before returning to normal operations.

In addition, if your Disaster Recovery Plan is focused solely on planning for potentially catastrophic situations, it may be too narrow to address minor (and more common) service disruptions that might not require relocation to an alternate site. Dependent on your court's needs, your may want to include several Disaster Recovery Plans in your court's overall BCP.

Summary

Although volumes of information have been written on the subject of disaster recovery planning, it is not always easy to find the information presented at a summary level. In that spirit, this article is written to outline key principles that will be helpful to you as you create an effective Disaster Recovery Plan for your organization's technology.

References

Rasmussen, Audrey. Disaster Recovery. Network World Network Systems. Management Newsletter. Network World, Inc., September 2001.

Knisley, Joseph R. Implementing a Disaster Recovery Plan for Telecom Systems. EC&M Magazine. Prism Business Media, Inc., August 1995.

Author

Pat Patterson, Chief Technology Office, Superior Court of California, County of Ventura.

Resource and Jurisdiction Contacts

Pat Patterson, Chief Technology Office, Superior Court of California, County of Ventura.

Approved by the CITOC Editorial Board on April 19, 2007