

Information Technology Disaster Recovery Planning for Court Institutions

By Judge Herbert B. Dixon Jr.

The courts serve a central role in our constitutional democracy. Under the rule of law, people rely very heavily on the courts and on courthouses, all of which are subject to various natural, technological, or humanly caused disasters or catastrophes. Preparedness for such events is a vital government function, but it is particularly important for the courts because they must remain open to the extent possible to ensure that all people's legal rights are protected.

—EMERGENCY MANAGEMENT IN THE COURTS: TRENDS AFTER SEPTEMBER 11 AND HURRICANE KATRINA.¹

Courts are dependent on digital storage of information, computerized case management systems, electronic filing and retrieval, and communications systems, the same as businesses, individuals, and other branches of government. When disaster strikes, however, whether natural or man-made, there is more for a court to resolve than finding a location to conduct trials and other court proceedings—much more!

If the truth be told, the multiple information technology (IT) systems in every court must have a disaster recovery plan for minor and major casualties, including

- Natural disasters: flooding, earthquake, lightning, storms, and tornadoes;
- Environmental and physical disasters: fire, heating/air-conditioning failure, power loss, loss of communication medium (e.g., a cable break), damage from broken water/sewer lines or fire alarm sprinkler system, and pandemic illness or disease; and
- Man-made disasters: intentional or unintentional destruction of a system or system component, lack of maintenance, hacking, and malware.

The above is not an exhaustive list of disaster possibilities. But, when a

catastrophe happens, a primary determinant of a court's readiness is whether sufficient forethought has gone into the process of recovering from such an abyss. At the risk of oversimplification, I offer this "CliffsNotes" of a disaster recovery planning process. Hopefully, this will cause those who have not thought about the possibility and effect of a natural or man-made disaster to start working on such plans for their court institution.

Although this article is intended to provide a few initial thoughts to the concerned chief judicial officer and court administrators about what is needed, all readers are cautioned to understand that the creation of an IT disaster recovery plan is an extremely complex, detailed, and technical exercise. The essential components of the disaster planning process discussed in this article are based primarily on a publication by the National Institute of Standards and Technology, namely, Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems* (NIST Planning Guide).² Notwithstanding that the NIST Planning Guide was prepared for federal government agencies, the National Center for State Courts notes that the publication provides extensive contingency plan guidance for IT systems and is an excellent resource for courts.³

Recovery Phases Following a Disaster

Whether the disaster is major or minor, the NIST Planning Guide notes three phases that must be addressed by the responsible parties in the disaster recovery planning process. First, there is the Activation/Notification Phase. As implied by the name, this phase involves activating the preestablished plan and notifying the disaster recovery team. Second, there is the Recovery Phase, which involves the recovery team identifying and prioritizing recovery activities, restoring operations at the same or an alternative site, and implementing any other applicable preestablished contingency plans. The third phase is the Reconstitution Phase, which involves restoration, testing, and validation of the system; returning it to normal operating condition; and preparing the system against future outages.

Since the Activation/Notification Phase involves activating the preestablished plan, obviously there must exist such a plan—a disaster recovery plan (DRP). So, the first thing that the chief judicial officer and administrators must do is commission the development of a plan.

A DRP, as discussed in this article, refers to the plan of action following a

major disruption to primary facility infrastructure. This plan is designed to restore operability of one or more information systems at an alternate site after an emergency. Generally, an IT DRP operates in conjunction with the overall Continuity of Operations Plan (COOP) for the court institution; however, a DRP may be used even when the COOP is not activated, as might be the case with fire or water damage confined to the computer room.⁴ Often the IT DRP is concerned with the procedures for relocation of information systems operations to an alternative location, after which the contingency recovery plan for each system would be implemented. A DRP may include contingency recovery plans for one or more systems. The recovery plan for each system may be activated in the current location or in an alternative location as determined by the DRP. Although the subject of this discussion is disaster recovery planning, the reader should understand that a DRP is composed of one or more contingency recovery plans for individual systems.

Develop a Contingency Planning Policy Statement

The first step requires court officials to create a Contingency Planning Policy Statement. This includes defining roles and responsibilities and the scope of the policy, i.e., its applicability to the telecommunications system, case management system, etc. Another aspect of step one is an inventory of IT hardware (including servers, computers, tablets, and smartphones), software and other applications, and digital information (especially case files involving active litigation, judgments, etc.). Furthermore, with respect to ongoing operations, the planners must establish resource and training requirements for a disaster recovery implementation team, testing and maintenance schedules for existing and replacement equipment, and the frequency of data and other information backups and storage. The contingency planning process must ensure that copies of program software are available at a safe location (i.e.,

a remote site unlikely to be affected by the same disaster, a storage location in the cloud, or the vendor) for the Recovery Phase during which the team restores operations at the same or an alternative site or otherwise implements the preestablished contingency plans. It cannot be overstated that the IT Contingency Planning Policy Statement must take into consideration other plans associated with the court's institution-wide strategy.

There are other necessary steps in the creation of a Contingency Planning Policy Statement that are highly technical and include a business impact analysis and establishment of critical recovery intervals, such as the maximum downtime that should be tolerated (i.e., how long can a particular court operation continue to function effectively without the supporting technology?) and the maximum time it should take to recover from the failure of a particular system.

Create Contingency Strategies

Contingency strategies are created for the purpose of mitigating the risk of an IT system disaster. The strategies include backup methods, including whether the backup is on magnetic disk, tape, CDs, or some other medium; the frequency and scope of backups, e.g., daily or weekly backup, and full or incremental (files created or changed since last backup) backup; and recovery methods to restore a system operation as quickly as possible. And, of course, the backup contingency strategy must include consideration of an offsite location that is unlikely to be affected by the local disaster.

Alternative Site

Admittedly, a major long-term disruption is a rare event, but facing a major disaster without a preestablished recovery plan would exponentially exacerbate the situation. A major disruption should be accounted for in the contingency planning process. For instance, an offsite facility some distance away must be considered so that the offsite location is unlikely to be affected by the same casualty that was experienced locally. Also, consideration must be given

to whether other local institutions have made arrangements with that same facility. Imagine the disastrous results if numerous local institutions made arrangements with the same alternative facility that is unable to accommodate all customers if that catastrophe affects enough of those customers simultaneously. This is the type of foreseeable problem that contingency planning is intended to mitigate.

Hardware and Software Acquisition and Replacement

A disaster in traditional terms means that onsite equipment is probably destroyed or unusable. An inventory must be prepared of the minimum equipment and software necessary to resume operations. Also, the process for acquiring hardware and software to resume the court's core functions requires specific attention. This process may include accessing equipment that was either stored in remote locations as a part of the disaster planning process or in active use in locations unaffected by the disaster. Additionally, as part of the contingency planning, service agreements should be considered with vendors for lease or purchase of software, replacement equipment, and emergency installations and maintenance. There should be sufficient geographic diversity among potential vendors to have a choice of vendors that are unlikely to be impacted by the same disaster, be it storm, earthquake, civil disturbance, or pandemic. Obviously,



Judge Herbert B. Dixon Jr. is the technology columnist for *The Judges' Journal* and a member of the ABA Journal Board of Editors. He sits

on the Superior Court of the District of Columbia and is a former chair of the National Conference of State Trial Judges. He can be reached at Herbert.Dixon@dcsc.gov. Follow Judge Dixon on Twitter @Jhbdixon.



The backup contingency strategy must include consideration of an offsite location that is unlikely to be affected by the local disaster.

cost-benefit considerations must be a part of this contingency planning process to work effectively with available personnel and within financial resources. The planners must recognize that an alternative site fully ready and prepared to commence operations may be financially prohibitive, and that consideration must be given for alternative site, equipment, and software plans of a bare-bones nature merely to get through the crisis until the local site can be restored.

Establishing Roles and Responsibilities

It is not enough merely to make contingency strategy plans for information backup, alternative sites, and hardware and software acquisition and replacement; the planning must also include designated teams to implement the various strategies—teams that are trained and ready to respond to the minor or major incident that has triggered implementation of the DRP. These teams may include, but are not limited to:

- Management team,
- Outage assessment team,

- Operating system administration team,
- Server recovery team,
- Local area network/wide area network (LAN/WAN) recovery team,
- Database recovery team,
- Network operations team,
- Application recovery team,
- Telecommunications team,
- Testing team,
- Physical/personnel security team, and
- Procurement team.⁵

Moreover, the DRP and its included strategies must recognize the possible need for multiple teams performing similar functions, for example, specialized application and software systems that each needs its own dedicated team. And, assuming the occasion for activating the team is a disaster that disrupts communications through normal office channels, the disaster recovery team coordinators must have alternative means to contact members of their teams, such as home address, cell phone, personal e-mail, and contact information for a close friend or relative that is likely to have access to the member.

Testing and Training

Each discrete part of the DRP should be maintained in a state of readiness. This includes having trained personnel ready to fulfill their roles and responsibilities within the plan. Testing of the systems should occur at regular, predefined intervals to ensure that the plan is not deficient or outdated and to confirm the accuracy of the process needed to recover each system that has suffered from the disaster disruption. Indeed, the disaster recovery implementation team must test the various systems after recovery to ensure that a DRP has performed as expected. In this regard, end-to-end disaster recovery exercises should be considered to provide a realistic readiness status and bring out any complexities, intricacies, or imperfections in the plans for recovering multiple systems in the case of a widespread catastrophe.⁶ Thorough preparation and coordination involve a great deal of planning from all the participating teams. “Mini” tests and some end-to-end testing of various components will give the best opportunity of identifying potential issues before they occur and provide

some reasonable basis to assure the adequacy of the DRP for multiple systems.

Training for each person assigned disaster recovery implementation responsibilities is critical to ensure that each member of the team is prepared to participate in testing, simulated exercises, and, should the worst happen, actual disaster recovery implementation.

Plan Maintenance

The overall DRP itself must be maintained in a constant state of readiness. Each part of the plan, for each system, must be regularly reviewed and updated to ensure that new information is documented and that up-to-date contingency measures are in place. The DRP is not an autonomous plan. It is interrelated with the court's overall COOP, and a change in one IT system or element might affect another IT system or some other part of the institution. Accordingly, the plan must be reviewed frequently for accuracy and completeness at an organizational and institutional level, including the plan's part within the institutional COOP. Whenever changes are made to the plan, they must be fully

tested, and training material and DRP documentation must be updated. It is essential that formalized change control procedures be adopted and maintained under control of the IT department and the IT DRP coordinator.

Distribution of each aspect of the DRP must be carefully considered. Each coordinator for each system covered by the DRP should have a copy of the plan. A copy should be stored at the alternative site (if an alternate site is predetermined), at a secured location onsite, and at a secured offsite location (i.e., perhaps where the backup data and information are stored). Also note that the plan, or parts of it, may contain sensitive operational and personnel information, in which case the planning process should ensure the protection of that sensitive information.

Conclusion

As mentioned at the beginning of this article, the creation of an IT disaster recovery plan is an extremely complex, detailed, and technical exercise. This article is not intended to outline all the steps that are necessary to create an effective DRP.

However, this article is intended to encourage discussion about the process to develop such a plan so that the courts are ready to protect the community's legal rights, even during the time of a catastrophe. ■

Endnotes

1. T. Birkland & C. Schneider, *Emergency Management in the Courts: Trends After September 11 and Hurricane Katrina*, 28 NAT'L CTR. FOR STATE COURTS JUSTICE SYS. J., no. 1, 2007.
2. NAT'L INST. OF STANDARDS & TECH, NIST SP 800-34 REV. 1, CONTINGENCY PLANNING GUIDE FOR FEDERAL INFORMATION SYSTEMS (NIST PLANNING GUIDE), available at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.
3. NAT'L CTR. FOR STATE COURTS, A COMPREHENSIVE EMERGENCY MANAGEMENT PROGRAM: A MODEL FOR STATE & TERRITORIAL COURTS 28 (2007).
4. *Id.* at 27.
5. NIST PLANNING GUIDE, *supra* note 2, at 26.
6. S. Subramaniyan, *How to Conduct an "End-to-End" Disaster Recovery Exercise in Real Time*, DISASTER RECOVERY J. (Apr. 3, 2013), <http://www.drj.com/articles/online-exclusive/how-to-conduct-an-end-to-end-disaster-recovery-exercise-in-real-time.html>.