

Disaster Preparedness

Disaster Recovery

scheme, design, contrive, organize, systematize, methodize, rationalize, centralize, order, program, propose, suggest, resolve, intend, project, aim, approach, approach a problem, confront a problem, attack a problem, make (or draw up) a plan, conceive (or form) a plan, draw up, draft, frame, shape, form, work out, map out, lay out, sketch, sketch out, chalk out, design, design a prototype, program, lay the foundation, lay the cornerstone, map out a course, mark out a course, shape a course, schedule, draw up a schedule, phase, adjust, revise, redo, recast, improve, prepare, arrange, prearrange, predetermine, think ahead, look ahead, calculate, budget, forecast, predict, foresee, envision, expect, follow a plan, have a policy

Disaster <noun>

1a. An occurrence inflicting widespread destruction and distress.

1b. A grave misfortune; great or sudden misfortune; catastrophe.

2. *colloq.* complete failure.

A publication of
LawNet, Inc.

January 2001

Disaster



A Note from the Editor

*"Life is what happens to you while
you're busy making other plans."*

~John Lennon

Disasters can strike at any time and most generally occur with little or no warning. As information technology and financial professionals, a large share of the burden for planning for disasters and certainly recovering from disasters falls to us.

This white paper presents several articles that focus on preparation for and reaction to disasters, ranging from the annoyance of hardware failure or data corruption at the low end to the devastation of full-scale physical destruction of facilities at the other. One piece is written from the perspective of a colleague who has lived to tell the tale -- a real-life account of recovery from the destruction of a tornado.

We gratefully acknowledge the experience, expertise and professionalism of our authors and hope that you find many pearls of wisdom herein.

Randi Mayes
LawNet, Inc.

Disaster Preparedness
Disaster Recovery

Contents

Business Continuity Program: A Necessity for a Law Firm2
by Atlas Lee, Shook, Hardy & Bacon L.L.P.

Disaster Planning: Developing an Electronic Vital Records Program7
by Beth Chiaiese, LegalKEY Technologies, Inc.

When Good Data Goes Bad13
by Randy Steere, Independent Consultant

**The Law Firm of the Future:
 Architecting an Information Infrastructure**18
by Lynn Marquedant, EMC Corporation

Just Another Day: Tales of a Texas Twister21
by Tony Lansford, Shannon, Gracey, Ratliff & Miller, LLP

Our Sponsor

This publication is sponsored by EMC Corporation. At EMC, we build the world's most robust, secure and trusted information storage infrastructures. Our storage systems, software, networks and services ensure fast, round-the-clock access to all of the information businesses and individuals must have to prosper in the Information Economy. Every business—in fact, every organization—runs on information. Extracting maximum value from this information requires an E-Infostructure™, uniquely provided by EMC. E-Infostructure is a shared foundation of technologies, tools, and services that enables a business to live inside a web of networked, constantly available and accessible information. Our job is to help law firms transition from where they are today to where they need to be, when they need to be there. EMC's E-Infostructure is the only foundation flexible enough to help them make the vertical leaps necessary to not only stay in the game, but to get ahead and win.

Disclaimer

This report is designed for use as a general guide and is not intended to serve as a recommendation or to replace the advice of experienced professionals. If expert assistance is desired, the services of a competent professional should be sought. Neither LawNet, Inc. nor any author or contributor shall have liability for any person's reliance on the content of or any errors or omissions in this book.

Copyright Notice

Copyright© LawNet, Inc. 2001, All Rights Reserved. Printed in the United States of America. No part of this report may be reproduced in any manner or medium whatsoever without the prior written permission of LawNet, Inc. Published by LawNet, Inc., c/o Randi Mayes, 2110 Slaughter Lane, #115-149, Austin, TX, 78748.

About Our Authors

Atlas Lee

Atlas Lee is the Director of Business Continuity for Shook, Hardy & Bacon L.L.P. in Kansas City, Missouri. He is a Certified Business Continuity Planner and holds a Bachelor of Computer Science Degree. He has ten years experience in Business Continuity and fifteen years experience as a manager in Information Technology. Atlas can be reached at alee@shb.com.

Beth Chiaiese

Beth Chiaiese, CRM is the Director of Education and Outreach for LegalKEY Technologies, Inc. During her 22 year career, Ms. Chiaiese worked as a records management consultant, assisting law firms throughout the country with the selection and implementation of records management software, process reengineering, and the development of records, conflicts and docket/calendar policies. She is a frequent speaker on law firm records and information management topics, appearing at these national conferences: the American Association of Law Libraries, LawNet, Managing Electronic Records (MER), and ARMA International. Ms. Chiaiese is also currently co-authoring a textbook tentatively titled: Records Management in the Legal Environment, to be published by ARMA International in 2001. Ms. Chiaiese is a Certified Records Manager and holds a Master's Degree in Library and Information Sciences. Beth can be reached at (773) 205-5822 or by e-mail at bchiaiese@legalkey.com.

Randy Steere

Randy Steere was the IT director at the Connecticut firm of Shipman & Goodwin for seven years. He is currently self-employed as a consultant to law firms and other corporations using the CMSOpen accounting software from Solution 6. As a consultant, he helps firms with all aspects of their accounting, conflicts, records, calendaring and marketing needs at both the technical and strategic levels. He also sells a highly customized Executive Inquiry System to firms using the CMSOpen software. Randy has a Masters in Computer Science from Rensselaer Polytechnic Institute specializing in databases along with two additional Masters degrees in Music and Divinity from Yale University. While employed by his firm, Randy was active in LawNet in a variety of volunteer positions and has been a presenter at numerous LawNet conferences. Randy can be reached at Randy535@aol.com.

Lynn Marquedant

Lynn Marquedant is an Industry Marketing Manager at EMC Corporation. With over 12 years in the IT industry, Lynn has spent the last 5 years focused on the specific issues of information storage. Lynn holds a Bachelor's Degree in Biology and Chemistry from the University of Vermont and an MBA from Babson College. She can be reached at (508)435-1000 x75702 or by e-mail at marquedant_lynn@emc.com.

Tony Lansford

Tony Lansford is the Director of Information Technologies for Shannon, Gracey, Ratliff & Miller, LLP, a 50-attorney firm in Fort Worth, Texas. Tony has served in that position for five years, and worked for an insurance warranty company as Computer Services Manager prior to joining the firm. Tony has been active in LawNet and ALA. His hobbies include golf, fishing and traveling. Tony can be reached at tlansford@shannongracey.com.

Business Continuity Program: A Necessity for a Law Firm

by Atlas Lee

Shook, Hardy & Bacon L.L.P.

Disaster Preparedness
Disaster Recovery

Obtaining the authorization to initiate a disaster recovery plan can be next to impossible for some organizations. But it was not for Shook, Hardy & Bacon L.L.P. In the summer of 1990, an explosion and subsequent fire in downtown Kansas City, Missouri, knocked out power to a very large portion of downtown where our corporate offices are located. Of course, this severely impacted a number of our critical business processes, thus forcing us to realize the necessity of being protected from a serious business interruption. Immediately thereafter, thanks to the commitment and consent of our senior-level management, we were authorized to start a program to protect the firm from such interruptions.

I had unofficially managed the business continuity/disaster recovery effort since 1990, along with my official role of Information Technology Manager. It should be noted that in 1990, we had approximately 500 employees, three offices and two mid-range computer systems and a very simple Local Area Network and Wide Area Network architecture. Now we have close to 1,800 employees, 13 locations, over 170 servers and mid-range computer systems and a very complex Local Area Network and Wide Area Network architecture. Also, I now have a staff that consists of a Business Continuity Specialist and two Computer Security Analysts who have the responsibility of Business Continuity Planning, Emergency Response, Disaster Preparedness, Auditing, and Computer Infrastructure Security.

This article has been written to assist you in developing a Business Continuity Plan by providing a framework and methodology used by many of the prominent Business Continuity and Disaster Preparedness/Recovery centric organizations.

What I have to say is not all-inclusive or all-encompassing, but I hope it will help you maneuver down the right path of implementing a viable, successful plan to restore your firm's business processes in the event of a serious business interruption. Even though it may seem like a daunting project, it does not have to be. You may initially be the sole owner of the project with overall responsibility, but remember you can start small. Some key items that may help you keep that focus:

Review What You Currently Have in Place

- Daily full image magnetic media backups are recommended because of the increased time it takes to restore incremental backups. Files, save sets, databases, etc. should be restored from tape periodically to confirm the integrity of the backup.
- If you don't already use a vendor that has a secured, environmentally-controlled offsite storage site for your magnetic media and vital records, I highly recommend it.
- Do you have redundancy built into your computer infrastructure? This could be UPS for your critical hardware components, an electrical filtering system to ensure "dirty power" does not get through to your critical systems, and mirrored and/or hot swap disk drives to make sure that a failed disk drive does not take down a critical application for an extended period of time.
- Review of your firm's insurance policy to make sure it has adequate "Business Interruption" and "Out-of-Pocket-Expense" riders. You want to make sure that "Standard Care" was taken or "Due Diligence" was exercised if you have to mitigate the effects of a business interruption on your firm's critical business operations.

Plan Initiation

For an individual tasked with the responsibility of providing the firm with computer network or other service area support, a business continuity program can be an arduous task. You might know the importance of having such a program in place, but the decision-makers have to have the facts in order to implement the program. Their question will be, "why?" This is because the program is often looked at as an expense and not a revenue generator. Needless to say the cost of not doing it greatly outweighs the cost of doing it due in part to the following:

Your firm has a professional obligation to protect the assets of clients and the firm.

Your firm may have statutory obligations in correlation to work being done for a client.

Your firm has an ethical obligation to ensure the best interest of not only your clients but also the employees of the firm.

Your firm has a moral obligation to the well-being of the employees who have supported the organization.

Additionally, communicate the need for a continuity plan by raising the level of awareness of senior-level management regarding the ramifications of not having a comprehensive plan to address potential business interruptions, such as:

Lost revenue

Lost Customers/Clients

Negative Publicity

Loss of Business

Loss of Competitive Edge

After a serious business interruption:

Over 40 percent of businesses never reopen.

A company that experiences a total computer outage that lasts more than ten days will never recover financially.

50 percent will be out of business within five years.

After you have successfully persuaded senior-level management of the necessity of having plans and processes in place to address any potential business interruption, then you should address the following.

Assign a person the responsibility of managing the effort. Senior-level management must appoint someone to lead the business continuity planning effort that has the power to lead, influence, support, prioritize, and organize the project. Senior-level management must provide full support to the project team, and mechanisms should be developed to keep the senior staff informed of the business continuity planning project status. Senior-level management will play a key role not only in approving continuity strategies for critical business processes but also in deciding which processes are critical and must be planned for.

Identify key, reliable personnel as team members with the understanding that you have a cross-mix of practice section, business unit, and information technology personnel to cover all areas that may be affected by a serious business interruption. Whenever possible, the project team should plan to empower employees during the implementation of the plan to strive to eliminate situations where centralized execution takes place.

Contract external personnel if needed. It is key to making sure your program gets off on the right track. You may want to contract the initial phase to a business continuity consultant or an organization that has expertise in business continuity planning and/or Disaster Recovery services. If outside consultancy is obtained, their role should focus on facilitation, not project ownership.

Acquire appropriate hardware and software for this project. It is suggested the hardware consists of at least a mid-range performance laptop (for mobility) with a small high-speed printer. Software should be a universal word-processing application, but preferably a business continuity planning software application developed by organizations such as Comdisco, SunGard, or Strohl Systems.

Other references and recommendations about hardware, planning software and other related Business Continuity topics can be found on the Disaster Recovery Journal Web site, which is www.drj.com or on the Contingency Planning and Management Web site, which is www.contingencyplanning.com.

Evaluate and Identify Risks

Determine the probability and consequences associated with potential risks to your firm. Identify controls and safeguards to prevent or minimize the effects of a business interruption.

Have or gain knowledge of the physical and computer security access and controls in your firm. Have or gain knowledge of the facilities infrastructure of your firm.

Seek external assistance, such as a Business Continuity consultant to "jump start" your program because often you will not have the personnel resources to adequately initiate the program.

Prepare a risk analysis that includes a broad range of possible business interruptions, including natural, technical, social, and human threats. Each functional area of the firm needs to be analyzed to determine the potential impact associated with different disaster scenarios such as: geographical location, proximity to major transportation arteries, history of the location's susceptibility to natural disasters, etc.

Provide for the worst case scenario: destruction of the main office. Rather than attempting to determine exact probabilities of each business interruption, use a rating system spanning from high to low to include a mid range to identify possible threats.

Determine the probability of occurrence and the potential impact of each type of threat on the various business units and practice sections within the firm.

Identify the preparedness and preventative measures, if any, already in place. Once the potential areas of high exposure to the individual business units and practice sections are identified, additional mitigation measures can be recommended.

Have senior-level management determine their acceptable risk level. Their acceptable risk level will most likely determine the overall resources and cost dedicated to this effort and then:

Identify risk reduction alternatives.

Identify vulnerabilities/threats and exposures.

Understand the loss potential from natural, man-made, accidental, intentional, internal, and external risks. This is especially important if you have offices in multiple locations and overseas.

Determine the firm's vulnerability to the aforementioned loss potentials.

Perform a Business Impact Analysis

The Business Impact Analysis, more commonly known as a BIA, is important because it makes the person in charge or his/her designee who is responsible for a practice section or business unit determine what is critical to his/her respective section and what is not. This very often necessitates a collaborative effort between the Business Continuity person(s), other members of the practice section or business unit, and individuals in departments that work closely with the practice section or business unit, because they may be adversely affected either collaterally or residually.

A Business Impact Analysis identifies the critical business processes that most affect the firm's revenue and assets. This process helps you to identify and prioritize the recovery strategies that might be needed during an extended business disruption. A Business Impact Analysis is also a comprehensive process that defines your critical business processes and the resources needed to support them. It is very important to address both internal and external processes. A frightening fact learned by a number of firms during the Year 2000 planning phases was our total dependency on the utilities, the court system and some vendors.

Identify the individual or group of individuals who needs to provide you information. These individuals should have a broad knowledge of the practice section or business unit and are most likely to provide accurate and objective information regarding their practice or business sections. To be successful and gain the assistance that you require, senior-level management will have to reiterate to these individuals the importance of being selected and their responsibility to provide information that is requested of them in a timely manner. A request to participate in a Business Impact Analysis project that is mandated by senior-level management has a much greater chance of succeeding due to the reality that participation is required. One of the primary goals is to make sure everyone involved understands this is a team effort. This puts in motion the understanding that this is the most important phase of Business Continuity Planning. Communicating the seriousness of the process raises the level of overall awareness and helps create an atmosphere of teamwork, cohesiveness, and unity.

When appropriate personnel are identified, you must:

Explain the Purpose

Explain that you are there to help by getting their practice section's or business unit's relevant information for input to planning strategy.

Explain that the plan is not an information technology plan - but a plan to recover the practice section's or business unit's information technology capabilities.

Reiterate the importance of having a written plan in the event key people with all of the intellectual knowledge are not around.

Explain the Focus

Focus on the time-critical business processes (this is usually about one half of what they do).

Assume a worst-case business interruption (worst time of day/week/month, etc.).

Assume no recovery capability exists. Determine manual ways of getting the work done.

Remain focused on the scope of the Business Continuity Plan.

Explain the Type of Information Needed

Comparative information will be very beneficial.

Questions will be structured so there are no wrong answers.

Do not get sidetracked by insignificant information.

Document the Results

Begin documentation of the results immediately. Also, determine the format that you will use to prepare the documentation.

Develop individual business unit and/or practice section summaries if necessary.

Send early results back to interviewees for confirmation.

Present the Results

Draft the report to review internally.

Schedule individual senior-management meetings as necessary.

Prepare a presentation for senior-management to explain the scope, goals, and objectives of the project.

Distribute the report to all involved in the project.

The Final Product of a Business Impact Analysis

When done properly, the Business Impact Analysis sets the stage for producing the firm wide contingency plan by identifying the most critical business processes across your entire enterprise, barring subjective prioritization by practice section.

It helps determine the maximum outage that a business process can sustain before it severely impacts the overall operation of the firm.

It identifies the financial, productivity, and personal impacts of an extended business disruption.

It assesses short-term business impacts and potential permanent business losses.

It identifies the most vital records to protect.

It identifies which business processes and assets require the highest level of protection.

It takes into consideration the various methods of recovery strategies and alternatives.

It quantifies the financial investment necessary for the various levels of business protection.

Develop Recovery Strategies for Your Firm

Identify and understand all of your viable options to include:

The cost of your recovery strategy.

The advantages of your recovery strategy.

The disadvantages of your recovery strategy.

It helps to develop business unit/practice section consensus to determine the "best fit" recovery strategy.

Meet with the appropriate personnel in the practice sections and business units to identify viable recovery options. (This process was very successful during most Y2K-planning efforts.)

Consolidate all recovery strategies if applicable.

Identify alternate facilities and off-site storage requirements.

Develop manual procedures in the event there is a delay in becoming electronically enabled.

Develop reciprocal agreements with other firms or businesses, if there is no conflict of interest.

Identify alternate means of communications such as Internet, cell phones and two-way radios.

Prepare cost/benefit analysis for the agreed upon strategies.

Emergency Response

It is imperative that the safety and well-being of your employees is the highest priority. Ensure that updated emergency response procedures from the firm and building management are in place and easily accessible.

Preparing your personnel for emergencies can help diminish the effects of increased absenteeism, poor morale, lowered productivity, high medical and mental health claims, an increase in workmen's compensation cases, and possible litigation.

Make sure all employees understand evacuation procedures. Ensure evacuation routes are clearly marked. Ensure all personnel can be accounted for in the event on an evacuation. Determine a pre-assigned

meeting place in the event the building that you occupy has to be evacuated. Have periodic emergency response drills for fire, evacuation, bomb threats and common local emergencies such as tornadoes, earthquakes and hurricanes.

Ensure that methods of communicating are defined (cellular telephones, messengers, radio).

Personnel that are CPR trained and/or have completed Emergency Response training need to be identified. Ensure that everyone knows where medical equipment/treatment can be obtained.

Development of the Plan

Document vital applications and vital data sets.

Form disaster recovery teams. Work with the practice section or business unit supervisors to assign team leaders, alternate team leaders, and team members.

Develop immediate response, notification, and contact procedures.

Develop plan activation procedures.

Develop hardware, software, and telecommunications configuration documentation.

Develop vendor information including their after-hours and emergency phone numbers.

Develop a damage assessment methodology to ensure there is a plan to replace the most critical systems first.

Develop recovery procedures that are detailed enough that a system or process can be recovered fairly seamlessly, but easy enough that the average layperson can utilize it.

Develop plan distribution and control procedures.

Implement Corporate Awareness Programs and Training

Employee Awareness Training

It has been stated that employee awareness is the single most effective and, at the same time, least expensive countermeasure that a company can employ. It is imperative that the organization is aware of your Business Continuity program, especially the overall scope of the program.

Formal Business Continuity Planning training needs to be provided for the individual(s) intimate with the development and maintenance of the plan.

Team members must be trained and made comfortable with their roles.

Keep the firm apprised of the status of the project.

Remember that any training and associated awareness programs are ongoing.

Test and Exercise Your Plan

One of the worst things that can happen after you have developed and implemented your plan is to let it sit and grow dormant. Even though there are several methods of testing your plan which range from a tabletop walk-through to a full-scale disaster recovery deployment and the associated benefits, I have outlined the following as being extremely crucial:

Test your plan to verify its feasibility.

Test your plan to verify functionality and usefulness.

Test your plans so that team members can interact in a mock or real disaster situation.

Testing will reveal areas of weakness and vulnerability.

Testing will help redirect your focus.

Document test results.

Analyze test results with appropriate personnel.

Make necessary adjustments to your plan.

Maintain and Update Your Records

Schedule regular plan reviews with applicable section, business unit, and team member personnel.

Make necessary changes as often as required, but at least quarterly.

Make sure you have audit and control procedures in place.

Make sure that recipients acknowledge receipt of all updates.

Conclusion

Although law firms generally are not mandated to have Business Continuity or Disaster Preparedness/ Recovery plans in place, the call to have or not have one is subjective but paramount. The facts regarding the consequences of not having a plan in place are well documented. In a number of disastrous events, some high profile companies have been financially crippled or put out of business.

It should also be noted that the notion that a business interruption will never happen to "us" is a very sad commentary on the state of business interruption preparedness for many businesses, especially law firms.

Please make sure you are prepared!

Disaster Planning

Developing an Electronic Vital Records Program

by Beth Chiaiese, CRM
LegalKEY Technologies, Inc.

Disaster Preparedness
Disaster Recovery

Law firms and legal departments are information-centric organizations. Like other businesses, they are administratively dependent upon internal information for operational, fiscal, legal and strategic decision-making purposes. This information must be immediately accessible to firm administrators to ensure the ongoing operation of the firm, and to provide the infrastructure on which the firm fulfills its primary purpose - client representation and service.

Lawyers provide services to clients based on information they gather, which, when synthesized with their expertise, results in a record of decisions, events and other activities that memorialize the work done on a legal matter. Therefore, rather than producing a tangible product, the lawyer's work product consists of recorded information in varying formats - electronic and hard copy, documentary and graphic. The lawyer refers to this work product throughout the course of a legal matter. An inability to access it jeopardizes the client's legal and financial position, and thus jeopardizes the firm.

It is critical that the firm resume meeting its clients' needs as soon as possible after a disaster occurs. Even though the firm has experienced a disaster, it is possible and probably likely, that the entire business community has not. This is certainly true to the extent that many law firms represent national and international clients. The client's business and litigation activities are ongoing, and the lawyer cannot afford protracted down time from his/her efforts to effectively represent the client's interests.

When a disaster occurs that prevents a law firm from accessing either client-based or administrative vital information, it cannot function. The loss of information to a law firm is therefore potentially more damaging than the loss of the firm's office space or physical equipment. Therefore, a necessary component of a contingency and business resumption plan for a law firm is a program that defines and protects the firm's vital records. Vital records are defined as:

... records containing information essential to the survival of an organization in the event of a disaster, . . . [regardless of] medium. Such records are necessary to continue operations without delay under emergency conditions. They contain information necessary to recreate an organization's legal and financial position and to preserve its rights and those of its employees, customers and stockholders.¹

What are the law firm's vital records? Clearly they include a subset of the administrative records that the firm needs to continue internal operations. These include billing and accounting records, payroll records, contracts and partnership records. However, they also include client/matter records - those records that have been traditionally found within the physical file the firm maintains for each matter on which it works.

Law firms have always considered the client/matter file to be paper-based. Thus it exists as documents filed within classified folders that are stored in a central records center or in a lawyer's office. It is not uncommon for a large law firm to have thousands of active files, each of which potentially contains hundreds of documents. To designate the client/matter file as a vital record requires some method to create a back up copy of the file, which is then accessible after a disaster. Most law firms do not have the resources to copy each active file, store the copies offsite, and update them regularly. Instead, to the extent that law firms have given any consideration to the protection of vital records, they have relied on the ability to recover client/matter documents from other sources, such as the court, co- or opposing counsel, or the client itself.²

Although it is certainly possible for a firm to reassemble client/matter vital records by collecting them from outside parties, it would take most firms many months to recreate the records for their active matters. This paper demonstrates that this effort is no longer necessary. By relying on technologies that most firms already have, it is possible to identify administrative and client/matter vital records, to create or capture them electronically, and to retrieve them far faster than by recreating physical copies. By developing a formal vital records policy based on electronic records, the firm will be able to resume client service almost immediately after a disaster occurs.

This article will define the steps a law firm should undertake to establish a formal vital records program based on electronic records. It will then discuss how the firm can use existing technologies to ensure that all vital records are captured electronically. This technology includes records creation and capture applications, but it also includes using an electronic records management system as a tool to identify, schedule and locate vital records so that they can be recovered as soon as a disaster occurs.

The Vital Records Program in a Law Firm

A vital records program is "... a set of policies and procedures for the systematic, comprehensive, and economical control of losses associated with vital records."³ A law firm attempting to develop such a program should follow these steps:

- Establish the program.
- Identify the vital records.

- Evaluate the risks.
- Protect and update the records.
- Implement the plan.

Establish the Program

Most law firms have not undertaken a formal methodology to create a vital records program. Although in general law firms have recently spent a considerable amount of money upgrading their technology infrastructure, they have spent little effort developing policies for the use of information. Many law firms do not have formal records retention policies, e-mail management policies or disaster plans. To the extent that these types of policies exist, they are confined to the mechanics of backing information up, and destroying e-mail at defined intervals, with little thought about the content or nature of the information being destroyed. The fact that most firm's IT departments perform regular backups of information, which are then stored offsite, seems sufficient for the purposes of recovering information after a disaster.⁴

Because the senior management of the firm is ultimately responsible for losses experienced by the firm in the event of a disaster, it is critical that it mandate and support the vital records program. Without the support of the firm's senior management, lawyers, other firm administrators and staff will not provide the input necessary to define the program, nor will they have an incentive to support the program after implementation. However, it is likely that some member of the firm's information management team will need to educate the executive committee, managing partner, risk management attorneys, and chief administrative officer about the nature of potential disasters and the firm's potential risks.

Within the context of vital records protection, the two most critical members of the firm's information management team are the records manager and the firm's chief information officer or information technology director. These two individuals should assume responsibility for educating senior management and for developing the vital records program. The CIO has the skills and resources necessary to capture, back-up and administer electronic vital records. The records manager has the skills to undertake the fact-finding necessary to identify, classify, and schedule vital records for update. Other team members might include additional department managers and practice group representatives, or the process can occur within the context of the firm's technology committee.

The first task of the vital records team will be to develop a written directive that acknowledges the critical nature of the firm's information resources and which defines the need for a vital records program. The directive will be issued on behalf of firm management, thus providing the validation necessary for the next steps of vital records identification, risk analysis, protection and program implementation.

Identify the Vital Records

The vital records team should engage in fact-finding on both the administrative and practice sides of the firm to determine which records should be classified as vital. This fact-finding generally takes the form of personal interviews with the records creators or survey instruments sent to records creators for completion. In general, interviews are considered the better fact-finding device, since they elicit more immediate and accurate information.

The vital records team should schedule interviews with administrative departments such as accounting and finance, personnel, risk management, conflicts of interest, records management, docket/calendar, marketing and the library. On the practice side, the team should interview practice group directors or representatives. Because an individual practice group might include many areas of law, it might be necessary to interview individual practitioners, or groups of practitioners. Lawyers, paralegals and secretaries should be included.

Because staff departments or practitioners rely on a variety of records to accomplish their work, they are likely to believe that all of these records are vital. It is important to distinguish *important* records from *vital* records. Although important records facilitate the completion of a task, vital records are those without which a business-critical operation cannot be performed or which the firm is legally mandated to maintain. Therefore, current accounts payable records are vital, while records that support paid bills are important but not vital. Likewise, current client/matter files are vital, while closed files, which support completed legal matters, are not.

At the conclusion of the interview process, the vital records team should create a list of vital records, including these elements of information for each vital record:

- The name of the vital record.**
- The purpose of the vital record.**
- The reason why it is vital.**
- The department or practice area that creates and maintains it.**
- The medium in which the record is created and maintained.**
- The preferred method of protection.**

Administrative Vital Records

Each firm must define its own list of vital administrative records. However, it is likely that the list will consist of records that support the following:

- The financial position of the firm, *i.e.*, payables, receivables, taxes and partnership liabilities.**
- What the firm owns, *i.e.*, inventories of equipment, library holdings, or other physical assets.**

The firm's agreements with outside parties, *i.e.*, insurance policies, contracts, leases, and software license agreements.

Human resources, *i.e.*, payroll, benefits, partnership agreements and compensation, and recruiting.

Business processes of the firm, *i.e.*:

- o Conflicts and client/matter intake**
- o Docket/calendar**
- o Marketing**
- o Records management**

The information management environment, *i.e.*, diagrams of network configurations, specifications of computing platforms, backup strategies and inventories, master list of application software.

Client/Matter Vital Records

Each area of law will define specific vital records. For example, vital records for estate planning will include wills, codicils, asset inventories, or the formal estate plan. Litigation vital records might include correspondence between the client and lawyer, litigation strategy memoranda, pleadings, deposition transcripts or exhibits.

The interviews that the vital records team has with each area of law should focus on the specific documents necessary to protect the client's position, and to recreate the firm's strategy with respect to representation. The team should specifically focus on the need to preserve attorney notes as vital records - these are usually handwritten and not captured electronically. If a specific practice area indicates that these notes would be critical to the firm's ability to resume active representation of the client, a process must be developed to capture the notes electronically.⁵ The same is true of signed, original documents.

Evaluate the Risks⁶

A risk assessment is critical to the vital records program. It is important for the firm to determine which types of disasters it is likely to encounter and the specific risks these disasters pose to electronic records. An evaluation of the likelihood of certain risks helps define the specific methods used to protect vital electronic records.

Below is a list of potential disasters that can destroy or damage electronic records:

Malicious destruction or damage due to sabotage, viruses, terrorism and warfare.

Natural disasters, such as fire, flood, earthquake, violent weather.

Accidents resulting from carelessness or negligence, such as water damage, explosion, or fire.

Storage in improper environmental conditions, such as poor humidity or temperature control.

Over reliance on fire-resistant storage cabinets, which protect from direct flame damage, but not from heat damage to media.

Poor storage practices, such as careless tape mounting, failure to rewind, ineffective labeling, or failure to regularly test tape inventories and back-ups.

Hardware failure.

Malfunctioning software.

There are two types of risk assessments that the vital records team can undertake. A *qualitative* risk assessment involves an evaluation of the environment in which electronic records are stored, taking into account how the records will be retrieved and used. This type of evaluation will point out areas of potential risk that the firm can take steps to rectify. Areas of evaluation include security and access, password protocols, the use of surge and UPS equipment, fire prevention and control apparatus, back up procedures, and the likelihood of hardware and software failure.

A *quantitative* risk assessment estimates the likelihood of specific types of disasters and their impact on the firm's losses. The basic elements of such an assessment include a determination of the risk, the probability of such a disaster on an annual basis, and the cost of such a disaster. Again, such an analysis points out the appropriate priorities for the protection and recovery of vital electronic records.

Protect and Update the Records

Traditional (*i.e.*, paper-based) vital records methodologies called for protection by creating additional copies of the records. These copies were either deliberately made or were the natural result of a business process. The copies were dispersed to other locations, where they would be available for recovery after a disaster. To the extent that copies or the originals were maintained onsite, protective storage was used, such as fire-protected cabinets or vault storage. Finally, vital records were scheduled, so that older copies of records could be destroyed and replaced with current versions.⁷

Although most law firms do not have formal vital records programs, they do protect electronic information using methodologies based on these traditional principles. Law firm IT staff routinely rely on back-up procedures for electronic data and store these back-up copies offsite as a protective measure. Firms carefully select appropriate back-up media that satisfies requirements for long-term storage and restoration. If back-up media is stored onsite, protected cabinets and containers are selected.

In addition, IT staff uses technology to protect active (*i.e.*, not backed-up) records. Redundancy devices, such as RAID arrays, ensure that information can be salvaged in the event of a system crash. Virus protection software guards against outside corruption of

data. Password protocols and other security devices prevent unauthorized access to information.

Finally, some large law firms have designated and designed hot or cold sites that will ensure their ability to bring electronic systems on line as soon as possible after a disaster. Multi-office firms can designate another firm office as a base of operations after a disaster.

Because of these in-place strategies, law firm electronic records are already maintained in a current condition. To the extent that the firm's vital records are created within the firm's electronic environment, it should not be necessary to develop formal schedules to update them. However, there may be certain vital records that generate outside the firm. These might include contracts, payables, and records from parties received in response to subpoena. The vital records team must develop a process to capture these records electronically. A methodology to do this, using already existing firm technology, is discussed below.

Implement the Program

Implementation consists of obtaining management approval of the vital records program, publishing the program and training lawyers and other personnel. It also consists of routine audits to ensure compliance and regular updates of the program to ensure currency. Audit reports should be sent to senior management to evidence compliance and the overall effectiveness of the program.

Using Existing Technologies to Create and Manage Electronic Vital Records

Law firms routinely use technology to create and manage information. It is probably safe to say that most hard-copy records used by a firm are actually copies of records that originated electronically. Because of this, most law firm vital records are captured electronically in the ordinary course of the firm's activities. However, as mentioned, certain vital records originate externally and come to the firm as print records only. In addition, the signed and executed versions of certain vital records might need to undergo a separate capture process, even though the document originated using firm technology. Finally, to the extent that handwritten attorney notes are considered a vital record, they need to be converted to an electronic format.

The fact-finding exercises used to identify the firm's vital records reveal which vital records exist electronically and which do not. In order to implement a vital records program based on electronic records, it is necessary to capture those records that either did not originate within the firm or which have added content that does not exist electronically.

As will be seen below, firms routinely use a variety of records creation and capture technologies. The result is that many vital records already exist in electronic

form. It also means, however, that vital records reside in different native applications, which in turn reside in different locations. To ensure that the firm can locate all vital records quickly, it needs a cataloging system that tags records as vital and indicates their location. An automated records management system includes this functionality and, when coupled with the firm's strategies for back-up and redundancy, is the final technology that permits law firms to implement vital records programs based on electronic records.

Records Creation Technologies

Word processing

This is the most common records creation technology in the firm. Word processing software is used to generate most of the documentary records that populate both the client/matter file and the firm's administrative files. Correspondence, memoranda, reports, briefs and filed documents are all created using word processing software.

Process-based software

Firms use different application software to automate and manage administrative processes. The structured information in each of these applications serves as a record of the firm's activities, transactions and current position in its administrative areas. Post-disaster reports generated from these systems will enable the firm to reconstruct its operational position. Examples of these systems and the vital information they contain are:

Timekeeping, Accounting and Finance

Accounts receivable, payable and other financial information.

Human Resources

Payroll, benefits, other human resources obligations.

Conflicts of Interest and Client/Matter Intake

Status of potential clients and matters.

Docket/Calendar

Upcoming due dates.

Contact Management

Names and addresses of firm contacts.

Records Management

Catalog of firm's client/matter file holdings.

Inventory Management

Catalog of firm's physical inventory, including furniture, computers, printers, etc. Necessary for insurance claims.

Library Catalog

Catalog of firm's print library holdings. Necessary for insurance claims.

E-mail

E-mail is rarely viewed as a records creation technology, even though it is a pervasive communications medium that has almost replaced formal let-

ter writing in legal practice. As such it constitutes a significant repository of correspondence, and other records that should be included in both administrative and client/matter files.

Firms use other types of records creation technologies, including spreadsheet applications, presentation software, and database software.

Records Capture Technologies

Imaging is the most logical choice to capture non-electronic vital records. Today, most firms already use imaging technology for specific purposes. The most obvious example of this is litigation support software, which images produced documents, and then indexes them for retrieval.

The cost of imaging technology and storage has dropped to such a degree that it is now possible for law firms to consider expanding the scope of their imaging activities. Rather than restricting it to high-volume litigation matters, firms can consider using imaging to capture designated vital records. If the firm's vital records list includes documents that do not exist electronically, the firm should evaluate the cost of imaging these records, so that its vital records program can rely on electronic records.

Records Repositories

Because of the variety of technologies used by most firms to create and capture electronic records, they reside in a variety of native applications. This makes it difficult to segregate vital records from other important records. If a disaster occurs, it will be critical for the firm to locate and bring vital records online as quickly as possible.

One solution to this problem is to designate a single repository for vital records. To some extent this already exists in those firms that have implemented a document management system (DMS). These applications, which apply structured information to unstructured, documentary records, serve as repositories for records that have been created using standard records creation technologies such as word processing, spreadsheet or presentation software. The DMS can also serve as a repository for e-mail message and images.

The DMS however, cannot serve as a repository for reports that generate from process-based applications, unless the reports are converted to standard word processing or spreadsheet formats. Some firms have addressed this problem by placing the reports in a data warehouse; this solution requires an ongoing process to add current reports to the warehouse.

The combination of DMS and data warehouse will help a law firm locate its vital records in fewer places. However, since these repositories will hold non-vital records as well, the firm still needs a tool that will list and point to vital records specifically. This is the role of the automated records management application.

The Automated Records Management System

The automated records management system ("RMS") functions much like a library card catalog - it allows the firm to use structured data elements (metadata) to describe the firm's records holdings. The RMS imposes a hierarchical classification structure on records that links them to specific clients, matters and folders. Non-billable client/matter numbers can be created for administrative departments to allow capture of meta-data for the firm's operational records.

The RMS is a critical tool for the management and recovery of vital records. Functionality in these products permits the firm to describe its vital records at the document level. Specific metadata fields tag the records as "vital" and also indicate their location, which can be a physical space or an application path. In the event of a disaster, the firm's RMS can produce a listing of all firm vital records and their locations, to the extent that the firm has recorded this information in the RMS. Thus, the RMS is itself a vital record.

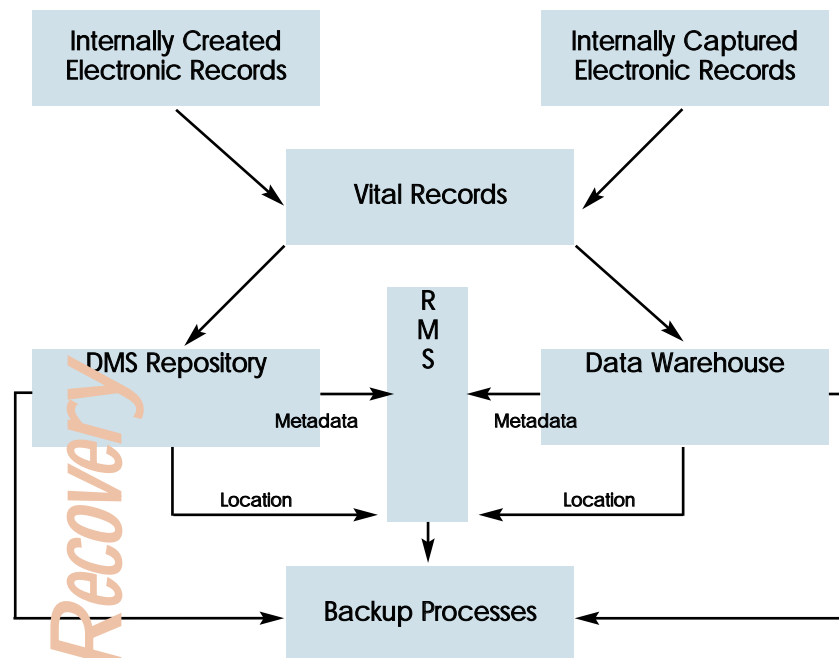
Current generations of law firm RMS products also enable the management of electronic records. Most law firm commercial products are integrated with document management systems and imaging systems, so that the DMS ID number or the imaging path can be entered in the location field of the RMS. Clicking on this field launches the DMS or imaging application, allowing the user to view the record.

It is also now possible for users to "declare" metadata into the RMS from the native application. This integration currently exists only with DMS products and e-mail systems, primarily Microsoft Outlook. Once the document has been created in the native application, the user clicks an icon, which allows already-defined profile information to be exported to the RMS.

Some RMS products take control of the declared record and remove it from the native application, preventing further editing and preserving its status as an issued record. The RMS can thus act as a records repository in the same way as a DMS or data warehouse. Because an RMS may not be able to capture records generated by systems such as process application software or non-word processing records creation applications, its use as a repository is limited.

Using the RMS as a centralized catalog of vital records permits the firm to quickly recover those records it needs to resume operations and client service after a disaster. Ensuring that these records have been created or captured electronically results in less down time during the recovery process. Using standard redundancy and back-up protocols means that copies of current vital records will be available for recovery.

This diagram illustrates how a firm, once it has taken steps to identify its vital records, can use existing technology to create, capture and recover the information it needs to survive when it encounters a disaster.



Endnotes

¹ARMA International, *Vital Records* (Prairie Village, Kansas: Association of Records Managers and Administrators, 1993): 1.

²This is a traditional method for protecting vital records. Called "routine" or "built-in" dispersal, it relies on workflow to generate additional copies of vital records that are then routinely sent to locations outside of a potential disaster site.

³William Saffady, *Managing Electronic Records*, 2nd ed. (Prairie Village, Kansas: Association of Records Managers and Administrators, 1998): 115.

⁴This conclusion is based on the author's experience consulting on records management issues in large law firms throughout the country. In addition, there is an absence of literature that specifically discusses the implementation of vital records plans in law firms. Therefore, the methodologies and recommendations in this paper have been extrapolated from records management and technology literature that describes the process in the general business community.

⁵Attorney notes capture a variety of information, some of which is not vital to ongoing representation. However, if attorney notes record strategy that is not formalized elsewhere, the absence of such information would jeopardize the firm's ability to resume representation after a disaster.

⁶Saffady: 129-137.

⁷ARMA: *Vital Records*: 5-6.

Authorities Consulted

ARMA International. *Vital Records*. Prairie Village, Kansas: Association of Records Managers and Administrators, 1993.

Gardner, H. Wayne and Brett Balon. "Disaster Contingency Planning." *The Records & Retrieval Report* 8, no. 7 (September 1992): 1 - 16.

Levitt, Alan M. and Karla H. Conford. "Contingency and Disaster Recovery Planning." *The Records & Retrieval Report* 7, no. 7 (September 1991): 1 - 16.

Muth, R. Timothy. "Electronic Disaster Planning for Law Firms." *Wisconsin Lawyer* 70, no. 12 (December 1997): <http://www.wisbar.org/wislawmag/archive/dec97/complaw.html>.

National Archives and Records Administration. *Vital Records and Records Disaster Mitigation and Recover: An Instructional Guide*, 1999 Web Edition. <http://www.nara.gov/records/pubs/vital.html>.

Phelps, J. R. "Setting Up a Disaster Preparation, Protection and Recovery Program for Your Law Firm." Law Office Management Assistance Service (LOMAS). <http://www.flabar.org/newflabar/memberservices/LOMAS/disaster.html>.

Saffady, William. *Managing Electronic Records*, 2nd ed. Prairie Village, Kansas: Association of Records Managers and Administrators, 1998.

When Good Data Goes Bad

*by Randy Steere
Independent Consultant*

*Disaster Preparedness
Disaster Recovery*

At the heart of the law firm, as with most businesses, is the intent to make money. It is the accounting system that tracks time and disbursements, produces bills, and collects cash. If this process stops for an extended length of time, the law firm goes out of business! While continuing to take care of the client's legal needs is clearly seen as a priority in a disaster, keeping the bills going out the door and the cash coming in is also very important for the ultimate survival of the firm. Even in a short-term "disaster", the firm must be able to incur expenses on behalf of the client, which usually means writing checks and handling accounts payable.

The accounting work consists of a number of time-constrained activities. Payroll must be met; checks must be cut; bills must be sent; deposits must be made, 1099 forms must be mailed and tax returns must be filed. In this regard, the accounting work is not much different from other areas of a law firm, except that those outside of accounting often do not realize the time-sensitive nature of this work until a deadline is missed.

The accounting software typically consists of both a database and the programs that access the database. We need to protect both of these software areas as well as the hardware and hardcopy paper that supports them. The accounting system is a transactional database, where most of the information relies on all the past history in the system. One can rarely restore one transaction or one table from a week or a month ago like one can restore an individual document from among millions at a firm. Unlike almost every other database in the firm, the accounting system must meet a much higher level of internal integrity that can hold up under the scrutiny of several yearly audits.

The author has witnessed widespread misunderstanding over this nature of the accounting database by both IT and accounting personnel, not to mention attorneys and other staff. One example on the IT side comes to mind often. After the IT personnel worked for a week to fix one corrupt table in the database constantly reassuring the accounting department that everything would be fine, the IT director announced that the easiest solution would be to "simply" restore the database back to the week before! Following efforts to resuscitate the accounting department, it was explained that they couldn't "simply" figure out what had

been done since the point of the proposed restore and "simply" re-enter all their work along with all the time entries made by the timekeepers. It ultimately spent a little more time and fixed the table.

Other examples from the accounting side usually center around a superficial knowledge of the database. One controller who had a basic knowledge of the tables in the system couldn't understand why all the transactions for one particular bill couldn't just be changed to correct a billing mistake. He was ready to update one table until it was pointed out to him how those transactions rippled through at least 19 other tables and affected balances for every month since the date of the bill.

The accounting system is probably the most complicated database the firm owns. It needs to be taken seriously by all involved, and it needs to be well protected. In addition, while not specifically addressed here, most accounting programs now contain other modules such as conflicts, records, marketing, calendar and other practice management systems. If this is the case in your firm, the protection of your accounting system takes on even more importance.

Certainly firms need to consider the entire range of insurance options to cover business interruptions, lost income and employee bonding for instance. While an important element in disaster planning, it is beyond the scope of this white paper to delve into the details of such insurance policies.

Central to this paper is the internal practices and procedures that need to be in place to ensure that the work of the accounting department can be recovered in the event of a disaster. We will proceed by examining the spectrum of possible losses that might occur - from the mildest to the most extreme.

Perhaps the mildest "disaster" for accounting would be for the system to be "down" for a short period of time. Nothing is lost, but nobody can work on the system until it is made available again. Such a scenario could happen for many reasons. Perhaps the network went down, a long upgrade had to be performed or the database server hardware crashed. Depending on the time period involved, this may mean writing manual checks, tracking cash receipts manually so the money can be deposited in the bank, and perhaps creating manual bills to clients. Despite having to catch up when the system becomes available, such an interruption can be survived for brief periods of time.

Having physical supplies on hand to get through the down time is important. Many firms use blank check stock and rely on the application to print checks, including the MICR encoding line. A supply of pre-printed checks should be maintained that can simply be filled in with a typewriter or by hand. Many firms also rely on the application to print the firm's letter-

head in lieu of pre-printed stock. A supply of pre-printed bill and reminder statement stock should also be maintained. It would also be helpful to have a few forms ready for manually tracking checks and cash receipts. This would ensure all the needed information was captured in an appropriate format for easy data entry later on.

Some firms have looked at clustering technology to minimize such down time, but, in the author's opinion, this is not yet robust enough to meet the stringent requirements of an accounting system. More than any other database in the law firm, the accounting database is totally reliant on what is known as the "ACID" properties of **Atomicity, Consistency, Isolation and Durability**. Without going into all the technical details, an "atomic" transaction guarantees that all or none of a declared transaction (one transaction could involve thousands of rows in many tables) will occur and that each transaction will occur in the exact sequential order that it was submitted to the database. Thus, if something happens in the middle of executing a transaction, that transaction would be completely rolled back as if it never happened along with every other transaction that hadn't completed. If two transactions access the same data, one is always blocked until the other one finishes to ensure the sequential order is preserved.

Paying the same bill with two client checks or cutting two firm checks with the same check number are only two examples where maintaining the sequential nature of accounting transactions is crucial. It is the database which ensures that an invoice isn't paid twice by two different accounts payable staff or that two of the firm's bills don't have the same bill number. For clustering to work, not only must the database match the highest level of transactional protection in any cluster cutover, but the accounting program needs to know about and be able to handle such an event. The seamless cutover simply doesn't exist at this point in time.

Rather than cluster their accounting servers, many firms have a backup database server on hand. It can be used for testing and running reports on a regular basis and if the primary server goes down, it can be pressed into service with relative ease. This solution is not for the brief and occasional interruption described above, but is an excellent foundation for disaster planning. This scenario brings us to the next level of "disaster" that could happen, one that would require a restore of the database and possibly a restore to a different server.

If the system goes down in such a manner that the database must be restored to either the same or a different machine, then another layer of concern enters the picture. There are a number of scenarios that could cause this to happen besides physical devastation from fire, flood and earthquake: corruption in the database, catastrophic loss of disk drives, upgrading

to a new machine or major hardware problems with the database server to name a few.

Restoring the database from a backup means understanding when the backup was taken, and re-entering any work that was lost. For the reasons outlined above, restoring the database almost always means restoring the entire database. Of course this raises the issue of the firm's backup strategy. Most all firms will do a complete backup of their accounting database every night. Most will take at least one tape weekly to off-site storage. In addition, most firms will perform a special "month end" and "year end" backup to be stored off-site and possibly restored into a "reporting" database.

Backup strategies are fairly routine these days, and this article won't address details, but there are some important considerations for accounting systems we must cover. Saving a "month end" and "year end" backup tape is a great idea in general. However, one needs to remember that as the software is upgraded and database changes are made, those backups may not be usable by the accounting software across upgrades. Most likely the reports could be run, but even this outcome is not guaranteed, and the firm needs to consider underlying version upgrades and their effect on the database and reporting. Indeed, the reports themselves may have changed and may not run accurately against older instances of the database!

Thus, having backup tapes of the database is probably not enough for your firm. It is necessary to store backups of the application files as well. Certainly as soon as an upgrade is performed, a complete backup of both the database and program files should be made in order to establish a new base-line for any possible restore. In this day when applications are highly user-customized, firms tend not to consider their own customizations as an "upgrade". Changes to reports, bill formats, user-defined fields, stored procedures, views, triggers, and user-defined tables should all be considered an "upgrade" in the sense that they should be logged and backed up.

The author has experienced many situations where a firm claims a bug in a report has mysteriously crept back into their system. Usually IT has restored the file server without alerting accounting or being aware of the fact that files on the file server may be constantly changing. From their perspective, they may only be tracking release upgrades from the vendor without taking into account what the firm itself has changed. Reports and bill formats are the most common examples. A log must be kept to correlate when upgrades and other changes (database or files) were made to specific dates and backup tapes.

Obviously, if a restore is necessary, one wants to restore the absolute latest backup. Most newer accounting systems use a relational database and

therefore have the ability to backup the transaction log throughout the day. The transaction log is a log of everything that happens within the database. This log can be re-applied to a full backup in order to "roll forward" transactions that occurred after the full backup. If a full backup was performed the night before and the transaction log was backed up at noon, then one could restore the full backup and apply the transaction log to restore all transactions that happened in the morning. Daily transaction log backups need to be part of every firm's backup strategy.

Most database products have certain commands that are not logged and therefore invalidate the transaction log. It is important for firms to understand the database product they are using and ensure that the backups and logs are restorable. In addition, all backup tapes have a limited life and need to be replaced on a regular schedule. Just because a backup process completes doesn't mean the data is actually on the tape. Restoring the month-end tape into a different database at the end of each month is an excellent way to test your restore capability.

Because databases in general are rapidly increasing in size, many database products now allow incremental backups. This is much like backing up only those files on a file server which have changed since the last backup. It is quite different from a transaction log backup. In the author's opinion, an incremental backup should never be used for accounting databases as the probability of error and failure is too great. The author has yet to see an accounting database, even in the largest of firms, that will not easily fit onto one tape backup. Entire backups should be performed every night.

If a restore to a different database server is required, it is also important to have all the server information necessary for a successful restore. There are many items to worry about:

1. Does the backup server have sufficient disk space, and is the configuration of those drives adequate to hold your database? The parameters of the database server itself need to be known. Most databases require server level settings to be identical in order to restore a database from a different server.
2. Are all the user logins established on the new server, and are they in sync with the old server? This concern applies not only to passwords but to the users themselves. What users have been added or deleted to the main server that have not been replicated on the backup? In many databases there are two records for a user, one at the server level and the other at the database level. These two records must link to each other. Thus, the server level record must match between the two servers. However, one cannot typically backup and restore server level data-

base information, and it is certainly not included with the database backup!

3. What does it take within your accounting system to point all your users to a different server, possibly with a different TCP/IP address? Alternatively, what must happen to take your old server offline and rename your new server to be identical to the old one?

Clearly, it is best to practice this scenario on a regular basis. You don't want to be learning how to install and configure a database server and have to add hundreds of users to the new server in the middle of a crisis! It is important to document your server, including all updates and hotfixes applied to the server itself.

Technical considerations for restoring the database are not the only considerations to worry about. If a restore is necessary, the accounting department will have to reconstruct information that was entered into the system after the point of restoration. This most likely includes time, disbursements and bills - items which would probably affect everyone in the firm. Very few firms have sufficient recordkeeping to cleanly reconstruct all activity from one or more days, to say nothing of a week or a month! Maintaining archives or hard-copy of disbursement imports, time sheets, bills, invoices, bank statements and checks at least for a certain length of time could come in very handy.

Equally important is understanding how to avoid the disaster in the first place. The most likely hardware failure to force a restore is a disk drive failure. If something other than the disk drive fails, most likely it can be repaired, and the system can be brought up again. However, if one of the disks fails with no redundancy, then the data is lost.

For this reason, various RAID (Redundant Array of Inexpensive Disks) configurations are usually used to provide pretty good safeguards against data loss. However, many a firm has been caught in a situation where a drive went bad and no-one noticed. Eventually other drives failed and the safeguard had been lost. The moral of that story is to be sure to monitor your hardware to catch failures before the redundancy also fails!

Other than hardware failure, the most common reason for a database restore is corruption. While database vendors assure everyone that the relational "atomic" functionality guarantees the integrity of the database, we know that in reality there are many reasons a database can become corrupt. A corrupt database means that some part of the internal structure of the database has gone bad. Rows within a table have become separated from the table; indices return wrong information; pointers within the database point to invalid places; these are all examples of a corrupt database. Some corruption can be repaired while other corruption cannot. Generally speaking, the end

user does not have access to these internal structures and therefore has limited means to repair them. A good analogy would be for someone to try to repair a corrupt Word or WordPerfect document. We have all seen plenty of examples of both that are simply beyond repair!

The best way to safeguard against corruption is to check the integrity of the database on a regular basis. All relational database products and most other database products have utilities to do this. Most firms will want to perform these checks on a nightly basis. More importantly, most firms will want their staff to review the results of these checks immediately!

The author has seen too many firms that didn't bother to check the results at all or didn't realize they were looking at old results because they assumed the integrity checks were running automatically when they weren't. One firm went several months without looking at the results and ended up restoring from a backup that was several months old because all the intervening backups were corrupt as well. It was many additional months before they were back to normal again. If your database is corrupt, you must restore from a backup that is not corrupt! Successfully backing up the database does not mean that it is not corrupt. One must understand that the corruption is merely being backed up along with everything else.

Last but not least is the scenario where both hardware and software are lost in a catastrophic failure. This scenario enters the realm of a complete disaster probably affecting much more than just the accounting department. All of the issues raised above apply. Given the existence of a good backup, the main issue is how long will it take to be up and running again. In the case of moderate down time, the most important information for day-to-day operation would be AR, WIP and payroll. Many firms keep well-catalogued binders of month-end reports that would help in this scenario. However, it is surprising how many do not safeguard those reports in any way. Many times they are sent off-site only after they are several years old.

Clearly, in the case of a more classic "disaster" such as an earthquake, fire, flood, hurricane or tornado, arrangements should be in place for working from a "hot" site or remote office. As firms become national and international in scope, having redundancy at another office is increasingly an option.

The absolute worst case scenario, which would be devastating to most firms, would be the necessity to completely start over from scratch. If everything were lost and no usable backups existed, the firm would have to start from an empty database and re-enter whatever information it could find. In this case, AR and WIP would be most important to begin with. The firm would have to make some strategic decisions as to the feasibility of recreating any history.

This article has dealt with various levels of "disasters" that might happen to an accounting department, from a minor system crash to a complete loss of data and everything in between. In the author's opinion, two major items have always surfaced in the face of a disaster. First, finding a good, usable backup; and second, having the knowledge to quickly get a second server up and running. While most firms handle the backup issue fairly well, the detailed knowledge needed to create a new server is usually lacking. Perhaps it has been years since the initial install or perhaps the person wasn't even at the firm at the time of the install. Regardless of the reason, firms tend not to invest enough in thoroughly training their personnel on the database system itself.

Having a spare server seems to greatly alleviate this second issue. Restoring the database to this server every month and having to work from this second database forces the staff to rehearse a recovery scenario. It also allows the staff to recreate this server occasionally without fear of interfering with normal operations. As a final word of caution, it should be noted that while catastrophic disasters such as floods, fire and hurricanes are rare, the author has tried to point out that most all of the disasters mentioned in this paper can happen from everyday problems as well. As such, they are far more common than firms realize.

Disaster Preparedness Disaster Recovery

The Law Firm of the Future

Architecting an Information Infrastructure

by Lynn Marquedant
EMC Corporation

Disaster Preparedness
Disaster Recovery

Information Storage Infrastructure Is the Key to Disaster Protection

We've all heard it said before . . . "Most of what lawyers do is paperwork." That paperwork includes researching legal precedents and preparing contracts and other documents. Paper accumulates with every deposition. One complicated case can generate thousands of pages of testimony. And all of this paper has to be read, analyzed, refined, and then stored into usable, searchable information. Add time, and this becomes a mountain of information - the storage, searching, and retrieval of which simply must be automated if any of it is to be used in the future.

What will tomorrow's legal services IT infrastructure look like?

How will law firms of the future be organized to best leverage their intellectual property?

And . . . Why is it imperative to start building a company-wide information infrastructure now?

Information Is Money

The successful digital lawyer is one who knows that he or she is in the information business as much as in the legal business, and that while automation often means that "time is money" in law practice, the more important insight is that "information is money."¹

Individuals and companies need specific knowledge that lawyers possess. Law firms, large and small, provide specialized knowledge in a variety of ways.

Recent advances in information technology are transforming the methods that lawyers use for processing knowledge and delivering legal services to clients. The information storage network infrastructure will become a critical tool in every aspect of law practice. The ability to share, manage, and protect legal knowledge on an information infrastructure will propel the forward-thinking law firm to greater success in the future.

IT Challenges Will Continue

As we venture into the new century, law firms will set out "to transform legal communications and transactions from paper-based to electronic-based systems in order to reduce costs and improve productivity, speed and overall effectiveness". This paper outlines the

¹Ethan Katsh, *Law In A Digital World: Computer Networks and Cyberspace*, 38 Vill. L. Rev. 403, 449-52 (1993).

information technology challenges they'll face and a three-phased approach to implementing and standardizing an information infrastructure - all to ensure the lawyers will have access to information at any time in the day or night and to ensure they are protected in the event of a natural or man-made disaster.

Today's law firms have an amalgamation of disparate technologies and a limited number of IT personnel. The most common IT challenges include the need to:

- ~Integrate heterogeneous information sources, including public records data and scanned images,
- ~Support heterogeneous platform access including Windows 3.1, 95, 98, and 2000, UNIX, and Linux,
- ~Control costs and maximize efficiency,
- ~Enable the use of information sharing standards such as the XML Court Filing Standard,
- ~Ensure consistent service, high availability and disaster protection to lawyers, clients, and courts, and
- ~Support expansion of their business

Time is of the essence. The majority of today's firms will continue to face these information technology challenges through the 2000's. The pro-active law firms - those that start to architect an enterprise-wide information infrastructure now - will be better positioned for future growth.

Online Applications Will Drive the Law Firm of the Future

The law firm of the future must support new on-line applications while at the same time ensuring compatibility with the firm's traditional e-mail, billing and project management applications.

Electronic filing will streamline the traditionally resource-intensive process of managing legal documents through litigation. With electronic filing, documents are shared over a computer network at the touch of a button instead of photocopying and hand-carrying legal documents between lawyers, clients, financial institutions, and any of a number of other interested parties. The law firm of the future will file legal motions to the courts and request the documents served to other parties all electronically over the Internet. Similarly, they will receive judges' orders and decisions directly on their computers.

Similarly, in preparation for taking legal action, the firm's attorneys and paralegals need electronic access to research past litigation, outcomes, and precedent history. They need electronic access to legal information either over the Internet protocol (IP) or via their Electronic Data Interchange (EDI) network. With electronic access to repositories of legal information, the law firm's personnel will perform more sophisticated searches in far less time than ever before.

And finally, with research completed and their litigation strategy in place, the law firm of the future will need electronic access to the court's case management system in order to schedule proceedings more quickly and efficiently. Lawyers and even clients may be able to schedule appointments in real-time without the overhead and time-delay of an administrator or intermediary.

The law firm of the future will need to support these new online legal service applications AND their existing e-mail and billing systems. Tomorrow's IT solution must be modular, adaptable, and flexible to grow in any direction the law firm, its partners, and large clients dictate.

Law Firms Will Implement Information Infrastructure in Phases

The law firm of the future will plan and manage the building of an information storage infrastructure in phases. Some firms will augment existing structures while others will completely re-engineer or outsource to run their business around the Information.

Recalling Professor Katsh's words " the successful lawyer is one who knows that he or she is in the information business as much as in the legal business", and given the continued shortage of IT staff, the law firm of the future will invest in and rely on a team of skilled IT personnel, without regard to where or for whom the individuals work. Instead, the successful law firm of the future will build a virtual team of IT expertise, assembled from in-house staff, consulting agencies, and vendor representatives. Following are the implementation steps that tomorrow's winning law firms will take to succeed.

First Step: Build the Foundation for Legal Document Archive and Retrieval

The first step is to consolidate and merge disparate information technology around a common storage infrastructure. Most law firms have acquired a set of heterogeneous platforms over several years - each time choosing the "best" computing platform for the new application. At some point, the law firm of the future cleans-up its datacenters, protecting the investment in as much of the existing equipment as possible, and connects its heterogeneous servers to a common repository of information storage. This becomes the foundation for legal document archiving and retrieval. Often the law firm will designate a master datacenter and one or more remotely located datacenters for disaster protection. The law firms of the future will install highly available and redundant disk subsystems in each location and connect them via high-speed channels to facilitate sharing, management and protection of the firm's business information.

Second Step: Create a Highly Available Environment to Attract and Retain Attorneys and Clients

With the information repository foundation in place and a high-speed channel connection between the datacenters, the firm of the future will install software to mirror (or make a copy) of the information between the two datacenters in order to assure business continuity. This means that no matter what happens to the firm's information at one site, the lawyers, clerks, and others can automatically access the other copy of information in the other site. They will be able to do this with little or no perceptible performance degradation so business will not be disrupted. The information storage network will be extendable to new lawyers and workers - located anywhere in the world- providing they have the appropriate security clearance.

To further protect the availability and the reliability of the information, the firm can install Input/Output (I/O) load balancing software on its UNIX and NT systems. This software will ensure that the firm's user requests for information get directed through the fastest path of access. This ensures a positive user experience. The lawyers and clerks at the firm, short on time, and long on pressing court dates and meetings and deadlines, will get to their information when they need it and ultimately will log more billable hours.

Final Step: Position for Future Growth with Modular Information Management

The successful law firm of the future will grow and change to leverage the value of their information. In order to manage the consolidation of their datacenter assets, ensure high service levels, and generally optimize efficiency, they will install storage management software. With this software they will monitor individual information storage device activity. They'll manage capacity and automatically re-allocate disk to support high-traffic applications and geographies.

One of the most far-reaching features of the information infrastructure is the ability to use software to save time. The law firm of the future will be able to generate new revenue based on the information infrastructure. For example, with state-of-the-art point-in-time copy software, copies of the information can be made available in different formats to clients and others in the supply chain. Real estate companies, for example need access to purchase and sales (P&S) agreements as do title and deed companies. The law firm of the future can store the master P&S, and then provide access to a copy to these other invested parties. The point-in-time copies will all be based on a single production copy of the information - to ensure consistency to these different groups of users. The law firms of the future will charge a fee each time an outside company wants access to their information; thereby further proving that "Information is Money".

For another example, using the point-in-time copy software, the law firm of the future will be able to off-load operational tasks such as backup and restore. The large volumes of legal information will never travel over the communications network, rather it will be backed

up off the "back-end" of the information storage network - through the high-speed channel. The result is that lawyers and clerks at the firm can still access the data at any time, day or night, and be assured that the data is fully protected and available.

Summary: Information Infrastructure Will Propel Law Firms into the Future

The law firm of the future that implements a modular, scalable information infrastructure will achieve numerous and measurable benefits from deploying a company-wide information infrastructure.

Major financial and operational benefits can be realized almost immediately. A network optimized for information storage will require fewer people to manage operations. Sophisticated replication software allows the law firm to "in-source" their disaster recovery contract at a considerable cost savings. They can achieve a measurable performance improvement by positioning legal information closest to where it is needed. Most importantly, by centralizing their critical business information and providing virtually continuous availability on a "24x7xforever" basis, the law firm of the future can grow rapidly, satisfy changing customer requirements, and generate new revenue while at the same time minimizing its risk and protecting itself from business interruption.

Summary of Benefits of Implementing a Firm-Wide Information Infrastructure:

Law firms can save system management costs by consolidating disparate datacenters and standardizing on an information infrastructure

Law firms can attract new clients and generate additional billable hours when more people can connect to the legal information more quickly.

Future law firms' IT departments will integrate heterogeneous information sources more easily and include access to court schedules and public records data.

The successful law firm of the future will attract more loyal clients and improve customer satisfaction because their information will be available when and where they need it.

The law firm is positioned to expand into new geographies, offer additional product lines, and enter new businesses by using and leveraging the legal information infrastructure.

Just Another Day

Tales of a Texas Twister

*by Tony Lansford
Shannon, Gracey, Ratliff & Miller, LLP*

I have been a lot of places and seen a lot of things. I have watched the cliff divers of Acapulco; I snorkeled with barracuda at Xel Ha in the Caribbean; I have even ridden an elephant through the northern rain forests of Thailand (a great time for anyone who likes that sort of thing). But on March 28, 2000, I was closely involved with something I never want to see again.

On that day at 6:30 p.m., Fort Worth, Texas was hit by a category F2 tornado. Our building, 35 stories of glass, was one of the hardest hit and has not been rebuilt yet. The owners decided it was too expensive to rebuild, cancelled all tenant leases and basically told everyone to find another place to do business.

I just want to share some of my experiences with you and some of the lessons learned about disaster recovery from a "seasoned veteran."

On Tuesdays I do volunteer work for my church in Dallas, about 30 miles away from Fort Worth. I left work early on the 28th as I normally do. About 7:00 p.m., I got a message from the receptionist's desk that said I needed to go home because all of my windows had been blown out by a storm. Now, this was one of those "grapevine messages" that somehow was twisted to sound as if my house was damaged. Mind you, I had no idea there had been a tornado at this point. I didn't even know who had left the message. My wife was with me, and my daughter was supposed to be at work. I tried to call home. No answer. I called a couple of people in the area. No problems as far as they knew. I then called our controller's home, and her husband answered the phone. I found out that it was she who called, that Bank One Tower had been hit by a tornado and that all the windows in the building were gone. Talk about a shock. I immediately left Dallas and headed for Fort Worth. I tried to reach our Administrator on the phone. My mobile phone couldn't make a connection to his home or his mobile phone. I tried several times and finally, by calling my brother in another town and having him connect via land line, I was able to get to our firm administrator, Mike. He, Susan our controller, Gloria our HR person and Jay our office manager had entered the building and were removing servers. I talked them through what to disconnect and what boxes to get while I was on my way downtown.

By the time I got there, around 8:00 p.m., all streets into downtown were blocked by police. I tried a couple of ways to get in and then remembered a seldom used street to enter from the east side of town. It was blocked by a policeman, but there was no other traffic. I pulled up to him and explained that I had an office in the Bank One Tower, and if I didn't get in there to get some things, our firm would be out of business. I was very surprised when he said, and I quote, "I'm not supposed to . . . but go ahead." I must have sounded sufficiently sincere that he knew our existence was in jeopardy. Anyway, I was able to get in and drive to within a couple of blocks of our building.

Disaster Preparedness
Disaster Recovery

I have to say that I have seen tornado damage on TV, and there were some members of our church that went to help with cleanup of the tornado that ripped through Oklahoma City, but to see the destruction in your own hometown is somewhat overwhelming. I parked in front of Chili's on Main Street. Glass and debris were everywhere. I was driving on a blanket of shattered glass. Ironically, when I opened the door of my automobile, I heard over the loudspeaker at Chili's "Jackson, party of two." They were still seating people. While two blocks away there was major destruction, most of the downtown area was intact with power still on and many people in the area.

I got out of the car and began walking the two blocks toward my building. The closer I got, the worse the destruction got. There were cars on their side. Most with windows out. In this area power was out, so lighting outside the building was almost nonexistent. The fire department and police were keeping people away, as there was still falling glass and other debris everywhere. This all was truly an amazing sight. But the worst was yet to come.

I got into the building and was met by building security. The maintenance manager, whom I know pretty well, was there; so I explained my purpose. Of course, they didn't want to let me up, but again I explained about needing to get things out. (They didn't even know that other people from my firm were there.) Again I was fortunate and was let up with a guard to accompany me. What I saw when I got to the 17th floor was simply incredible. I went through the door to our accounting department and was overwhelmed -- nothing was in its place. There were no windows. The wind was blowing the curtains. I climbed over the mess to get to my IT center. (The door off the hallway was blocked by debris.) As I walked through that door, I was taken aback. The IT room was completely destroyed. My office near the IT center had no windows. There was no ceiling. The light fixtures were all down. My bookshelves were in tatters. I had to climb over my desk to get to my files where I located my vendor file for Rental Systems, as I knew we were going to need PCs. My co-workers had already gotten most of the servers. Just as an aside, they were all still powered on. The power to the building had not gone off. The only server that had any real damage was my Exchange server, and it had taken a hit from something large and had been knocked on its side. We lost it; but all other database and file servers were saved. I did lose a network fax server, and we are still walking to fax machines. That's not a big deal in the scheme of things.

After gathering equipment, files and backup tapes I walked around a bit. All I could say was "WOW." You never think this could happen to you. I can't say that anymore.

After a night like that I didn't think it could get worse. At about 8:00 a.m. Wednesday morning, I got a phone

call. It was a secretary from a satellite office about 15 miles away that was connected to us via ISDN. The first thing she said to me was, "When am I going to be able to get on the network?" I was in shock. After a few moments of silence all I could think to say was "You have got to be kidding." This was the most absurd thing I have heard since "How do I turn on my computer?". I couldn't believe she thought the system would be back to normal that quickly. In fact, it would be about a week before we could get into some temporary space (a 10,000 sq. ft warehouse).

During the first week, I set up my servers (accounting and file serves -- as stated earlier, my Exchange server was gone) in my garage to test and to let our controller process cash and checks. Our staff was scrambling to find places to work. By the way, I would like to thank all in our area who offered space to our attorneys. We were spread in several directions. During that first week, I was putting files on floppy, e-mailing files to home addresses and generally looking like some sort of drug dealer, as we would have cars pull up to the house, come in for about 15-20 minutes and then leave.

Our vendors were great. I have one that provides printer services. They loaned us printers and copiers until we could get some of our equipment out of the building.

Our extra-contractual practice group was set up at a client's site. We rented PCs so they could work. We set up a small network using the client's backbone but were completely separate from the client's network on our own hub.

We were a fractured group but, all in all, a solid one. We all worked together to make a bad situation not so frustrating.

After the first week we set up shop in a warehouse. Yes, a warehouse for storing things. It was all we could find for such a large group on short notice. I set up several tables with workstations and printers that we were able to get out of the building. All systems were up and networked with our file server. Secretaries and lawyers worked from these workstations getting out product and keeping up with calendars and such. We didn't have an outside connection, so we were still isolated. A pain but still not critical. Most everyone setup e-mail on their own so they could communicate with clients.

I have to share with you the following. It is an excerpt from a letter dated April 4, 2000, from one of our partners to his clients

Our firm has had a disaster plan in place for many years, but fortunately we had never had to test it. Because of our wonderful staff, I am happy to report that it worked better than we could have imagined. The disaster plan calls

Disaster Preparedness Disaster Recovery

for our Accounting Manager to get current bank records and checks and leave the premises with them so they will be safe, and she did. The Executive Administrator is supposed to get our insurance policies and some other key documents and leave the premises, which he did. Our Information Systems Director is supposed to do a quick data back-up from the preceding midnight (our systems are backed-up at midnight each night) and leave the building with the back-up disks. However, he did not. Instead Tony, who is a giant-sized man well over 6 feet tall, simply got up from his desk, unplugged our network file servers and walked down about 18 flights of stairs with one under each arm. About an hour after the tornado destroyed our offices, our servers were up and running from Tony's garage without the loss of even a line of data. I probably don't need to mention that Tony is quite a hero around Shannon Gracey!

And then in follow up to his first letter he wrote a second one that is rather funny as well. The following is dated May 1, 2000:

Even without our paper files, we have been able to continue most of our work because we have had constant access to everything on the "hard drive" of our network. Had this kind of disaster occurred in the years before computers, I hate to think about the disruption in the lives of our lawyers and our clients. With the computer system, we have always had access to everything we produced and sent out - all we have been missing are the responses from the clients or the other counsel, copies of which are almost always available from their files.

And speaking of computers, remember Tony from my previous letter - our fabulous, giant-size Information Systems Director who lugged our servers out of the building immediately after the storm? One of my letters describing Tony's feat was sent to a Louisiana CPA with whom I frequently work. From there the letter somehow ended up in the hands of the new football coach at LSU. He sent an inquiry asking if Tony had any years of playing eligibility left! I think Tony is framing the letter for his new office in the UPR Plaza.

These letters are attributable to Phillip McCrury.

Needless to say I was appreciative of the kind words.

But I really do a back-up of the data and had the tapes. I had to go to them for the Exchange database that was lost when that server took a hit.

After setting up in the warehouse all went well, and we finally found some space in the building we reside in now and are in process of building out two new floors to move into permanent space.

This, in all, was an incredible experience where teamwork and a lot of effort was needed to keep the firm afloat. There is still much work to do and some changes to make in the way we handle disaster recovery. We have discussed this plan in many a meeting. It is not easy to just have computers, phones and people in place the next day after a disaster of this sort. I can only imagine what things would have been like if the tornado had been stronger. The building possibly would not even be there. Back up tapes should always be off-site, preferably in another part of town. (We follow this procedure, but the deposit box was in a bank just a few blocks away and was not immediately available either.)

We had, before this disaster, spoken with companies that offer space and computers for recovery at a cost for retainer. That may be great for large firms with large budgets. However, for us little guys (we have 50 lawyers), it was a stretch to keep that kind of plan within reach.

Again, I say this was a learning experience. We are still living out of boxes and using rented furniture, but we have all come out of this unscathed and with a better knowledge of what it takes to recover from acts of God. We had no control over this event, but the way we handled the situation demonstrates our character and resolve.

In many ways we are a better firm because of the disaster. If nothing else we got rid of a lot of paper we didn't need.

Paraphrasing the firm administrator when asked what his disaster recovery plan was, "Get up there and start getting stuff out."

That's what we did.

That's my story, and I'm sticking to it. Just another day in the life of an IT Director in Fort Worth, Texas.

