Wind, Rain & Fire: Disaster Preparation & Recovery

The Disaster Recovery Plan

The Florida Bar Annual Meeting
June 21, 2006

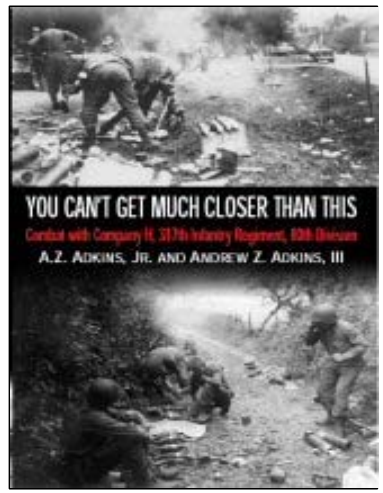
Andrew Z. Adkins III
Director, Legal Technology Institute
Associate Director, Technology Services
University of Florida Levin College of Law

Agenda

- Introductions
- Disaster Recovery Issues
- Disaster Recovery Scenarios
- Disaster Recovery Plans
- Practical DR Tips
- Questions

Andrew Z. Adkins III

- University of Florida Levin College of Law (1997)
  - Director, Legal Technology Institute
  - Associate Director, Technology Services
  - Adjunct Professor, *Law Practice Management*
- Legal Technology Consultant (1989)
  - 325+ Personal Consultations
- ABA TECHSHOW Chair (2000, 2001)
- LegalTech Conferences Co-Chair (2000-2004)
- Author:
  - *"Computerized Case Management Systems"*
  - *"You Can't Get Much Closer Than This"*
  - 125+ Legal Technology Articles
  - 130+ Legal Technology Presentations



Disaster Recovery/Business Continuity

Facts

- Business Continuity is a priority “issue”
- Planning and Preparations are significantly underdeveloped, underachieved

“Accidents and disasters do not make appointments.”

Disaster Recovery Plan Issues

- What's important to you?
- What's important to your staff?
- What's important to your clients?
- What's needed to keep the firm functioning?
- Who's involved in the DR planning?

"Disaster Recovery is MORE than technology recovery; it's also Business Continuity"

Disaster Recovery Plan Issues

- Who will initiate the plan?
  - Who will issue the order to “turn off” all servers?
    - May need to shut down servers to protect them
- Communicate this to everyone BEFORE you have to initiate the DR plan
  - Communicate how long servers expected to be down (if possible and in what scenario)
  - Eliminate the need to decide why, when, & how

Scenario Planning

- Possible scenarios:
  - Natural Disaster
    - Hurricane, Fire, Tornado, Flood, …
  - Man-made Disaster
    - Terrorist attack, Disgruntled employee, Lost Laptop, PDA (Stored Passwords)
  - Other Disaster
    - Entire IT staff “hit by a bus”

Disaster Recovery Plan Scenarios

- Data Stolen, Compromised
- Regional Office Destroyed
  - Regional servers destroyed or compromised
- Main Office Destroyed
  - Main firm servers destroyed or compromised

Disaster Recovery Plans – 1

- Contact Information
  - Who are the key people?
  - Who's in charge?
  - Where are they?
- Location Information
  - Where is the backup?
  - Where are the disks & license keys?
  - Where is the relocation site?
- Recovery Information
  - What is restored first?

Disaster Recovery Plans – 2

- List all technology assets
- List data backup information
- Identify Mission Critical Applications
- Identify Critical Data

Disaster Recovery Plans – 3

- What are your priorities?
  - Yes, this is a question for attendees

  1. Communications (phone, email)
  2. Data (firm, client)
  3. Web site

Disaster Recovery Tips – 1

- Plan on not having a full IT staff
  - They may also be personally affected
  - Look into outsourcing recovery “pieces”
- Your DR Plan should have a checklist to follow
  - The plan will be the voice of reason in a crisis
  - Test the plan at least once every year; this will help pinpoint problem areas
- Document everything you can during the recovery (contacts, meetings, dates, notes)
  - You’ll need this for insurance

Disaster Recovery Tips – 2

- Provide “main” players with the DR Plan
- Identify a “hot site”
  - Not necessarily a technology hub, but a “meeting place”
  - Copies of applications; license codes
- Leaders will look to the most prepared for support
- Communications (phone, email, etc.) WILL be overloaded
  - Phone book, includes work, home, cell, email(s)
  - Phone Tree

Disaster Recovery Tips – 3

- Keep an inventory of old computers, boxed up with CRTs, keyboards, mice, SW, image, Citrix (if used)
  - Store in a geographically safe location
- Keep old servers necessary for initial recovery
  - Store in a geographically safe location

Recovery Realities

- Day 1
  - Sympathy, compassion, concern
- Day 2
  - Assess status of technology & business
    - What works, what doesn't
    - Determine what part of DR Plan to put into action
      - This is why you discuss scenarios
    - Who's around & can work?
- Day 3+
  - Put the DR Plan into action
  - Rebuild communications first internal, then external

Recovery Expectations

- Lack of communications
- Limited bandwidth
- Limited resources
  - External as well as internal
- Displaced personnel

Lessons Learned (NO, NY firms)

- Blackberry chargers (left at office)
- High staff morale
- Gasoline shortage
- Delivery delays
- High level of vendor support
- Housing shortage (including hotels)
- Traffic problems
- After action meeting(s)

Questions

- What time is it?
- Do I know a good, *independent* legal technology consultant?

Thank You!

Andrew Z. Adkins III
Director, Legal Technology Institute
Associate Director, Technology Services

University of Florida Levin College of Law
PO Box 117644
Gainesville, FL 32611-7644
352.273.0765
adkins@law.ufl.edu
www.law.ufl.edu/lti