Disaster Planning and Security Issues

Catherine Sanders Reach, Director
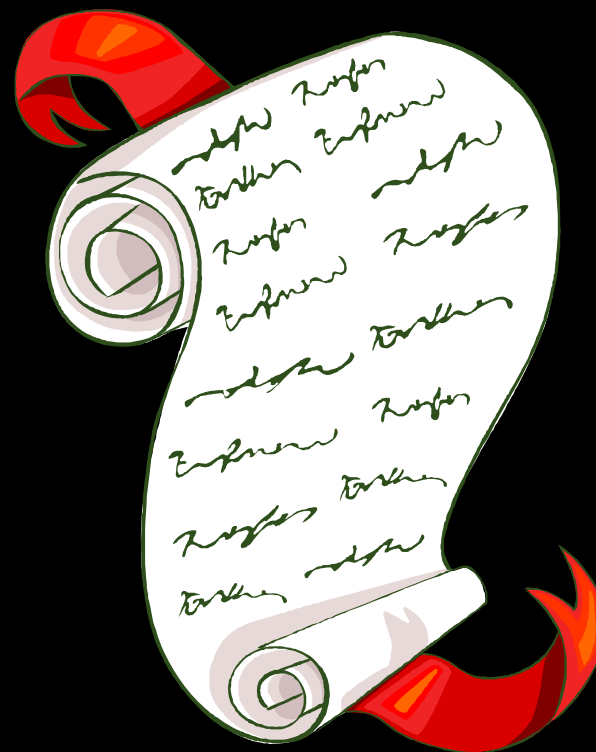
American Bar Association

Legal Technology Resource Center

July 27, 2006

A B A L e g a l T e c h n o l o g y R e s o u r c e C e n t e r

Today's Topics

- Disaster Planning

- Backup

- Security issues

Law Firm Disaster Plans

2006 Legal Technology Survey Report:

Does Your Firm Have a Disaster Recovery Plan?

	NUMBER OF LAWYERS AT ALL LOCATIONS					
	Total	Solo	2-9	10-49	50-99	100 or more
Yes	**53.8%**	57.4%	51.5%	44.0%	59.0%	59.0%
No	21.7%	38.8%	32.1%	16.9%	7.2%	1.5%
Don't know	**24.5%**	3.9%	16.4%	39.1%	33.7%	39.6%
Total	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Count	1124	258	305	207	83	268

A B A   L e g a l   T e c h n o l o g y   R e s o u r c e   C e n t e r

Disaster Planning

- Natural Disasters
  - Earthquake
  - Fire
  - Tornadoes
- Man-made disasters
  - Security breach or sabotage
  - Equipment Failure
  - Theft
- #1 goal (and possible ethical obligation):
  Get back up and running to serve clients

Planning for Disaster

- Written plan
  - Protect people
  - Protect business assets

- Model Plan
  - What must remain operational
  - Define each potential disaster and response
  - Be flexible and practical
  - Build in redundancy
  - Test Your Plan
  - Identify vendors to help with recovery in advance

Planning for Disaster

- Create a planning team
  - Review plan every quarter
  - Create and address scenarios
  - Be flexible
  - Assign tasks to people and have redundancy
  - Create a manual and make sure people have it and are aware of it!

Planning for Disaster

- Technology Considerations
  - Communications on overloaded or non-existent systems?
  - Copies of software licenses and installation discs
  - Store retired hardware offsite
  - Backup, backup, backup
  - Possible blog for communication?

Planning for Disaster

- Be prepared to be offsite

- Have contact lists:
  - Real estate agent
  - Insurance agent
  - Client lists and contact information
  - Recovery vendors
  - Attorney & staff external cell phone and email addresses
  - Court contacts

Backup

- Natural or man-made disaster?

- You need backup and a planned response!

- Backup media

  - High capacity tape, portable hard drives, online backup

    - Online backup has it's own risks

  - Backup servers, individual computers, peripherals

Backup Best Practices

- Full backup once a day

- Keep back up media offsite

- Test restoring the data

- Keep all software license numbers and installation discs

- Use Belarc Advisor to take snapshot of harddrives

Policies and Training

- Develop a security attitude

- Understand that restrictions and rules are for the safety of the firm and the firm's clients

- Stress security practices the same way you would with a child – "Stranger, Danger!"

- Your firm is your castle – lock the doors, bar the windows, and dig a moat

Policies and Training

- What security policies should be in place?
  - Computer acceptable use policy
  - Email use policy
  - Internet use policy
  - Disaster recovery plan
- Other useful, related policies
  - Employee privacy policy
  - Email/document retention policy

Policies and Training

- Make policies available
  - Shared network drive
  - Intranet
- Enforcement
  - Review and signed at least annually
  - Training sessions to reinforce understanding
  - Make FAQ available
  - Repercussions for non-compliance?

Physical Security

- Hardware is vulnerable
  - Laptops
  - Desktops
  - Servers
  - Storage devices (thumb drives, discs, etc.)
  - Cell phones and handheld devices
- What if anyone were to get unfettered access to any of these?
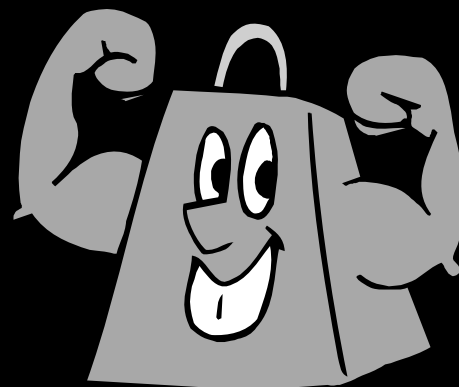
Physical Security

- **Laptops**
  - **Password at startup/password protected screensaver**
  - **Tether to desk (docking station doesn't count)**
  - **Use a non-descript travel bag and keep an eye on it**
- **Desktops**
  - **Password at startup/password protected screensaver**
  - **Tether/Secure**
- **Servers**
  - **Keep in a locked, windowless room with few access keys**
  - **Be aware of who has access to servers**
- **Storage devices (thumb drives, discs, etc.)**
  - **Password protect**
  - **Consider encryption**
  - **Keep an eye on them**
- **Cell phones and handheld devices**
  - **Password protect**
  - **Lockout after failed login**

Network Security

- Do not login as administrator, unless necessary
- Control file sharing
  - Disabled or read-only
  - Turn off file and printer sharing on your computer
- Install hardware firewalls
- Test vulnerabilities
- Protect at the server level – install security software to protect all devices on network

People Problems

- Outside the firm
  - Social engineering
  - Theft
  - Disposing of computers/devices/storage without wiping (not just deleting) the data
  - Your family (computer)
- Inside the firm
  - Disgruntled employees
  - Employees who are leaving
  - Untrained, unaware employees

Document Security

- Consider a document management system or case management system to control access to documents

- Deletion does not remove the document

- Levels of protection
  - Password
    - To open
    - To edit, copy, extract
  - Sharing
    - MS Office 2003 Information Rights Management
    - PDF – Portable Document Format
 - Encryption

Document Security

- Document Metadata
  - Library card for every document
  - Shows author, previous authors, editing time, tracked changes, versions, comments, and so much more!
- Just look under "Properties" tab or try enabling tracked changes
- Most prevalent in MS Office, but also in WordPerfect
- Getting rid of it
  - Tools from Microsoft
  - Save as PDF (which carries it's own metadata)
  - Third party software tools
    - Payne's Metadata Assistant, Esquire Innovations iScrub, Appligent GetMetadata for PDF
- Bar Associations are weighing in on this issue

Email Security

- The Threats
  - Spam
  - Phishing
  - Virus/trojans/worms/etc
- Your weapons
  - Updated, active antivirus software
  - Common sense and awareness
  - Spam filters
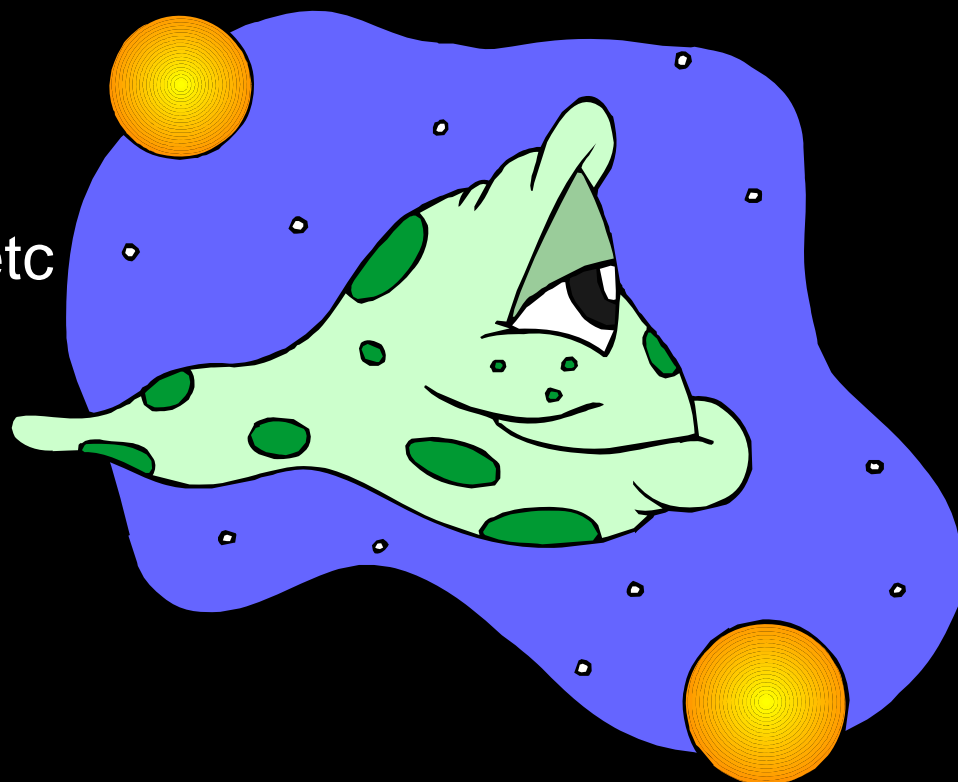
Email Security

- Fear of misdelivery
  - Double-check the to: cc: and bcc: before you send every time
  - Consider a privacy disclaimer at the beginning of the email message
- Password protect access to email programs
- Don't send anything you wouldn't want published in the <u>Fill-In-The-Blank</u>

Email Security

- For the firm website:
  - Using a separate email for website (lawoffice@) or a web form for general inquiries

- Separate personal from professional
  - Use a web-based account such as Yahoo! or Gmail for personal transactions – not your work email address
    - Helps identify spam and phishing messages in your work in-box

Internet Security

- The Threats
  - Spyware, malware, adware
    - Tracking cookies, keystroke loggers, rootkits
    - Zombification

- Your Weapons
  - Automate Windows Updates
  - Disable Active X in Internet Explorer
  - Use an alternative browser, like Firefox (but you still have to update IE)
  - Install software firewall, such as ZoneAlarm
  - Install anti-spyware, like PestPatrol or Spysweeper
    - Look for products that update themselves and protect, rather than just clean
  - Pop-up blockers

Wireless Security

- Wireless Networks
  - The Threats: Wardriving, nosy neighbors
  - Your Weapons:
    - Enable Encryption
    - Use hardware and software firewalls
    - Change all default settings
    - Limit the number of connections to the number of computers

Wireless Security

- WiFi

  - The Threats:
    Hackers/crackers,
    look-alike wifi networks

  - Your Weapons:

    - Resist using unsecured wifi networks

    - Use a VPN to get into your network

    - Use hotel/airport ethernet ports instead of wifi

Mobile Security

- Public PCs

  - Often full of spyware, like keystroke loggers

  - Is someone looking over your shoulder? (this goes for computing in any public place)

  - Do you want to have to remember to:

    - Delete cache, cookies, history, and offline files?

- Remote access to the firm

  - VPN (virtual private network) is expensive, but safest.

If Nothing Else...

- **Think passphrases, not passwords**
  - Strong passwords are over 8 characters long and contain a combination of symbols and alphanumerics
  - Example: "Mydoghasfl3as!"
- **Get security software bundles**
  - Combine antispyware, antivirus, firewall, privacy, intrusion detection etc. in one
  - McAfee, Symantec, Panda, Zone Alarm, etc.
- **Automate updates**
  - Antispyware and antivirus software that needs to be manually updated to be effective isn't worth the free pricetag
- **Security is up to you – not your IT staff or consultant**
  - Security is a process, not technology
  - Change your default settings
- **Do Not Get Gotten**
  - Read the End User License Agreement, be wary of offers that are too good to be true, don't click on pop-ups or blinking ads, realize companies do not ask for you to update your account information online (anymore at least), don't open attachments unless you know the sender and are expecting the attachment, be alert and wary

Questions?

See the webliography of security resources at:

http://www.lawtechnology.org/presentations/securityhandout.pdf

Catherine Sanders Reach
ABA Legal Technology Resource Center

sandersc@staff.abanet.org | 312-988-5053