Lawyers Mutual
www.lmick.com

The Risk Manager

A quarterly newsletter by Lawyers Mutual Insurance Company of Kentucky

SPRING 2011
Volume 22, Issue 2

The Legal Malpractice & Risk Management Conference Explores Technology Risk Management Issues for 2011

The 10th Annual Legal Malpractice & Risk Management Conference held in Chicago in February focused on the technology risk management issues concerning confidentiality and lateral hires. What follows is a recap of these conference programs intended to alert you to the risks and encourage a review of your firm's technology risk management practices.

23 SINCE 1987

"Passwords should be treated like your toothbrush – Don't let anyone else use it and change it every six weeks."

Anonymous

The Growing Threats to Client (and Firm) Data – Managing Technology to Meet the Challenges

This program began by stressing that the confidential data of law firms is facing security threats as never before. While this risk was once primarily a business risk of corporations, law firms are now a lucrative target of cyberscams. Especially vulnerable firms are those involved with mass class actions, high net worth clients, and the health industry (read personal injury medical records). Firm computer security is breached by tricking lawyers into downloading malware into computers and e-mail that infiltrates a system by bypassing technological network defenses.

Program materials included *Cell Phone Spyware Facts* that covers both cell phones and other covert law firm espionage techniques. What follows is a brief synopsis of this document and the panelists' discussion of it. *Cell Phone Spyware Facts* is available in its entirety on Lawyers Mutual's Website Home Page at *lmick.com*.

The technology threat to preservation of client confidentiality is nearly mind-boggling. Here are some of these risks:

Cell Phone Vulnerability:

- All cell phones can be bugged – every vendor is at risk.
- The smarter the cell phone is, the easier it is to bug.
- Spyware to bug cell phones is readily available on the Internet.
- It is possible to bug a cell phone remotely without the phone ever being in someone else's possession.
- Information that spyware programs can collect includes all conversations, contact data, multimedia messaging service, short message service, phone call history, e-mail history, webpage history, pictures, video, GPS location, cell tower triangulation history, and file system information.
- A cell phone can be programmed to act as a bug. For example, a person leaving a hidden cell phone bug in a meeting room can activate the phone to hear

continued

continued from page 1

meeting conversations. Similarly, a person attending a meeting with a cell phone bug with them can surreptitiously send meeting conversations to an accomplice in another location.

Unconventional Covert Espionage Techniques:

- Devices are concealed in fax machines that copy all faxed documents and download then to a remote location. This device is used to monitor conversations around the fax machine as well.
- A similar device is used in printers and copy machines.
- Shredders are bugged with a hidden digital scanner to copy and download shredded documents. One of these devices prints the document at the receiving location as it is being shredded.
- Tiny cellular bugs that are an entire cell phone are hidden in innocent looking appearing appliances such as a computer mouse, computer keyboard, table clock, and other objects that are connected to a live electric power source.

Is your cell phone bugged?

Cell Phone Spyware Facts lists these indicators that a cell phone may have spyware installed on it:

1. Battery warm when not in use.
2. Battery life is noticeably diminished each day.
3. Some Blackberrys: communication icon on right screen flashing.
4. Small pauses of audible communication while talking.
5. Light audible tones, beeps, or clicks throughout a conversation.
6. Flashing or flickering on display or change of brightness.
7. Some spyware programs require the spy to manually mute their phone; therefore, you might hear them in the background at the beginning of conversation or when they tap in.
8. Slower Internet access.
9. Suspicious third parties have detailed knowledge of your private conversations and locations (GPS).
10. You have opened a suspicious e-mail or one from a potential spy (allowing a Trojan Horse to install spyware remotely).

Countermeasures for meeting room security

There are a variety of ways of securing a meeting room. Examples are:

- Use a safe room for highly confidential meetings.
- Have qualified technicians sweep a meeting room.
- Allow no electronic devices in a meeting room.
- Use a cell phone detector.
- Employ a cell phone jammer.

Technical Surveillance Countermeasure Teams (TSCM) are available to audit security in a firm. While Lawyers Mutual does not recommend specific contractors, *Cell Phone Spyware Facts* includes information on how one TSCM company operates.

Laptop Security

Program materials offered this risk management advice for laptops:

1. Create firm-wide mobile device security policy and enforce it.
2. Don't take all information with you – just because you can doesn't mean you should.
3. Require strong two-factor authentication.
4. Encrypt all confidential data.
5. Never leave access numbers, passwords, or security devices in your carrying case.
6. Consider using a laptop tracking and wiping program.
7. Provide for physical security of laptops, including:
   a. Always keep your laptop in sight.
   b. Secure it when not in sight.
   c. Use a laptop security device.
   d. Use engraving or an asset tag to identify the owner.
   e. Be aware that computer bags attract undue attention.
   f. Watch your laptop when going through airport security.
   g. Never leave a laptop in view in a parked car.
   h. Secure your laptop in your hotel room when out of your room.

continued

"Computers are incredibly fast, accurate, and stupid. Human beings are incredibly slow, inaccurate, and brilliant. Together they are powerful beyond imagination."

Albert Einstein

continued from page 2

Developing an effective technology risk management program

Panelist Michael Downey of Hinshaw and Culbertson included his article *Serious About Confidentiality* (The National Law Journal, October 18, 2010) in the program materials. In the article he offered this advice for getting started in an effective technology risk management program:

1. Adopt clear policies and educate all personnel about the proper use and disclosure of client confidences, including to the media and on the Internet, and the consequences of noncompliance.

2. Purchase travel laptop computers and flash drives protected by full disk encryption, and insist that lawyers and staff use such protected devices when they travel with client-related or other sensitive information.

3. Ensure that all computer systems, scanner/copiers and smart phones that can send and receive data have password protections activated.

4. Ensure that people who have access to firm facilities and information can pass reasonable background checks and agree in writing to preserve confidences.

5. Keep the most sensitive information off the Internet, or at least secured on document-management systems.

6. Provide for secure disposal of confidential information at each workstation, as well as at copiers, printers and the like, and also for secure disposal of any computers (home or office) or data-storage devices that might contain firm-related information.

7. Assess whether the firm should purchase additional insurance or equipment to protect against data disclosure.

8. Plan now how the firm will respond to any disclosure that may occur, including how notice will be given to regulators, affected clients and the public, and what actions the firm will take to re-establish protection and sanction anyone who caused the disclosure.

What should a competent lawyer do?

If you are balking at the idea that you must implement technology risk management programs to protect confidential information, remember that the Rules of Professional Conduct on competence and confidentiality are more than a prohibition on revealing confidential information without client consent. A lawyer must also take reasonable care to affirmatively protect a client's confidential information. What may have been reasonable care a few years ago is no longer the case.

No matter the size of a law firm, affirmative action is required to avoid both malpractice and fiduciary breach claims because a firm failed to take reasonable care to protect confidentiality from a technology threat. Use the process recommended above to review your situation. Additionally, you may find these *Bench & Bar* articles on Lawyers Mutual's Website helpful in understanding and analyzing your technology risk management needs (go to *lmick.com* – click on Resources, click on *Bench & Bar* Articles, select article):

- The Amazing Client Electronic File.
- The Impact of the Internet on a Lawyer's Standard of Care & Professional Responsibility, Part 1.
- The Impact of the Internet on a Lawyer's Standard of Care & Professional Responsibility, Part 2.
- Lawyer Website Disclaimers - Fact or Fiction?
- E-Discovery Risk Management Is the "New New" Thing.

continued

2011 ANNUAL POLICYHOLDERS' MEETING

The Annual Policyholders' Meeting of Lawyers Mutual Insurance Company of Kentucky is scheduled for 8:00 a.m. EDT, Wednesday, June 15, 2011 in the Kentucky Room, Hyatt Regency Hotel, 401 West High Street, Lexington, Kentucky. Included in the items of business are the election of a class of the Board of Directors and a report on company operations. Proxy materials will be mailed to policyholders prior to the meeting. We urge all policyholders to return their proxies and to attend the meeting.

"To err is human, but to really foul things up requires a computer."
Arthur Bloch in Murphy's Law

High Tech Tools – and Traps – for Mergers and Lateral Hiring

As a Kentucky lawyer observed recently, layoffs of lawyers during the current economic decline resulted in making many good lawyers available for lateral hire in Kentucky. For this reason, the portions of the program *High Tech Tools – and Traps – for Mergers and Lateral Hiring* concerning risk management for lateral hires and departing lawyers should be useful information for Kentucky lawyers.

As a refresher, here are some of the risk management considerations for firms when making a lateral hire:

- Before hiring, screen candidates thoroughly by checking for:
  - o Legal qualifications – by getting authority to obtain information from law schools and bar admission and disciplinary authorities – trust, but verify.
  - o Ethics complaints and malpractice claims – inquire about potential claims.
  - o Financial status and credit record.
  - o Membership in organizations such as officer, director, or other interests in a business; and fiduciary services such as trustee, conservator, administrator, or executor.
  - o Powers of attorney held involving financial matters.
- After hiring:
  - o A firm lawyer should review every file brought by a lateral hire. Get client consent in writing before accepting a client's file brought by a lateral hire.
  - o Determine if the lateral hire has client funds and, if so, have them immediately deposited in the firm's client trust account.
  - o Inventory client property for which the lateral hire is responsible.*

** This list is derived in part from the following materials used in the ABA 26th National Conference on Professional Responsibility program On The Road Again: "Insurance Issues Related To Lateral Hire Musical Chairs," by Professor Susan S. Fortney, and the Alexander & Alexander article "Evaluating and Managing the Risks of Mergers, Acquisitions and Lateral Hires" edited by Anthony Davis.*

Program panelists emphasized that technology tools provide excellent ways to investigate and evaluate candidates, streamline the application process, consider conflicts of interest and screens, and ethically integrate into the firm client files, forms, and electronic devices such as thumb drives, laptops, and cell phones the candidate will bring to the firm. These tools includes electronic files management programs, conflict of interest programs, and Internet search engines. If technology is not used effectively in the hiring process, it can result in firm and public relations problems, and the Three "D"s – Disqualification; Discipline; and Disgorgement.

Technology tools are equally useful in out-processing departing lawyers by coordinating what client information, work product, and other documents may be taken electronically from the firm's IT system. The panelists stressed the importance of conducting an exit interview to assure that the departing lawyer and firm are in agreement on these issues.

The materials provided with the program included risk management guidance for these issues. What follows is a gloss of the key points:

Arriving Attorneys

Transferring Electronic Content to the Firm's Systems

Electronic Data Intake Acknowledgement

Before loading any electronic documents onto the firm's computer system, require the new attorney bringing paper and electronic documents to certify in writing that the documents and electronic files conform to the firm's guidelines for loading new documents on the system using an Electronic Data Intake Acknowledgement form:

Sample Form: This document acknowledges that I have been given a copy of the Firm's technology and data policies for arriving attorneys and have read and understood the contents. I agree to abide by the rules and procedures set out in these policies. I agree that the list below is a complete and accurate record of all data that I will be bringing into the Firm, and that all listed data meets the Firm's policies.

Signature _____ Date _____

Printed Name _____

Data Device (e.g. flash drive, CD)

Format (e.g. .doc, .pdf)

Nature of Data

continued

"Computers are useless. They can only give you answers."

Pablo Picasso

continued from page 4

Restricted Documents

A firm should not accept documents into its records system or computer system that are not documents of the firm's clients. Accordingly, attorneys who arrive at the firm from other law firms should not bring with them files, e-mails, or documents of clients of their former firm moving with them, unless and until the clients have cleared conflict checks. The firm should not accept documents that were removed from an attorney's prior firm without that firm's permission.

Approved Documents

Arriving attorneys may have personal specimens, exemplars, or form files that the attorney has developed. Such documents will be accepted provided they do not contain confidential information regarding persons or entities that are not clients of the firm, and provided that the documents are not the property of the attorney's former law firm.

Departing Attorneys

Frequently, attorneys leaving a firm for employment at other law firms require information about matters on which they worked to permit their new firm to do a conflict check. It is good policy to assist departing attorneys in performing conflicts checks in a manner that does not require disclosure of client-confidential information.

It is good policy to assist departing attorneys in performing conflicts checks in a manner that does not require disclosure of client-confidential information.

Because it may not always be known whether a particular matter on which the attorney worked was one that the client did not wish disclosed, the following steps should be taken in dealing with the departing attorney:

1. Produce a printout of the clients and matters on which the departing attorney logged time during the past five years (or shorter period during which the attorney was with the firm). Provide this printout to a partner designated by management in the practice group in which the attorney practiced for review for possible confidential matters (the "Reviewing Attorney"). Regarding departing summer associates, the Reviewing Attorney may be an associate.

2. The Reviewing Attorney will discuss the contents of the printout with the departing attorney so that the departing attorney will be generally familiar with the services performed. The departing attorney will be cautioned on non-disclosure of client-sensitive information, and will be provided a copy of the firm's policy for departing attorneys. With this caution, the departing attorney may be given a copy of the printout, and may make notes of the discussion.

3. The departing attorney should be instructed to ask the new employer to indicate for what clients he or she will be likely to be working, so that the attorney can determine whether work performed at the former firm conflicts with such representation. By approaching disclosure in this fashion, the attorney can avoid giving a detailed listing to the new employer of all matters worked on while at the former firm.

4. If the foregoing procedure is not satisfactory to the new employer, attempt to work with the new employer to assist it in performing its conflict check in a manner that will not require disclosure of client-sensitive information.

5. Upon request by an attorney who has given notice that he or she is leaving the firm, create a disk or other electronic media containing the following, which may be taken by the attorney leaving the firm:

- That attorney's Microsoft Outlook contacts.
- That attorney's Microsoft Outlook calendar.
- That attorney's personal Microsoft Outlook e-mail messages that they moved to a personal folder.

6. Departing attorneys shall not copy or remove electronic data from the firm's computer systems. Departing attorneys may request that electronic data other than those listed in the preceding paragraph be provided as well. The request should be directed to firm management for consideration.

continued

"Never let a computer know you are in a hurry."

Unknown

Lawyers Mutual
www.lmick.com

Waterfront Plaza
323 West Main Street, Suite 600
Louisville, KY 40202

PRESORTED STANDARD
U.S. POSTAGE
PAID
LOUISVILLE, KY
PERMIT NO. 879

Malpractice Avoidance Update

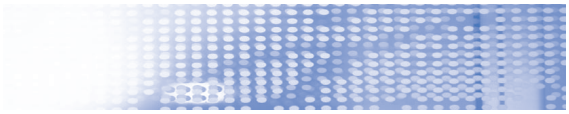
Member National Association of Bar Related Insurance Companies

For more information about Lawyers Mutual, call ***(502) 568-6100*** or KY wats ***1-800-800-6101*** or visit our Website at ***www.lmick.com***

continued from page 5

7. The departing attorney may not take:
   - firm training materials,
   - masters, forms or exemplars developed by or for the firm,
   - documents that contain or disclose client confidences,
   - documents that are subject to a protective order, or
   - client contact information other than client contact information contained in the departing attorney's own Outlook contacts file.

8. The exit interview of the departing attorney should include a discussion of the documents and electronic files that he or she proposes to take, and these parameters should be enforced at that time. The person conducting the exit interview may request to examine documents or electronic files being taken by the departing attorney.



A Client's Poem

If Only You'd Ask, I'd Be Happy to Say...

By Felice Wagner

If only you'd ask, I'd be happy to say
I wish you would do things more often my way.

If only you'd ask, I'd be happy to say
I don't like that new partner that calls every day.

If only you'd ask, I'd be happy to say
I'd like you to bill in an alternative way.

If only you'd ask, I'd be happy to say
We have four brand new this very same day.

If only you'd ask, I'd be happy to say
Responsiveness means calling back the same day.

If only you'd ask, I'd be happy to say
There are three other law firms in our lobby today.

If only you'd ask, I'd be happy to say
I expect your budget to reflect what I'll pay.

If only you'd ask, I'd be happy to say
When you go over budget, my career slips away.

If only you'd ask, I'd be happy to say
I wish you would do things more often my way.