Cyber Liability: Are You Aware of the Risks?

by Wendy F. Inge

An attorney's use of a computer tablet, a cloud based service such as Dropbox, a smart phone, a Wi-Fi network, a thumb drive, or even basic e-mail is not unethical nor a poor business decision. Today's technology driven world requires that lawyers and law firms take advantage of technology. Unfortunately, however, how the device or service is used can create security risks. Here are a few recent law firm examples.

- **Law Firm Website Defaced and E-Mail Hacked —** The hacking collective Anonymous defaced the website and broke into the business e-mail account of a Virginia law firm that represented a U.S. Marine accused of killing civilians in Haditha, Iraq. Anonymous accessed and eventually made public more than three gigabytes of data that contained court e-mails, faxes, and transcriptions related to the Haditha case. The only good news was that the firm's e-mail was not deleted by the hackers**.** The firm responded by reminding everyone that it is the client and witnesses whose privacy was invaded and who may be harmed by this rogue attack.

- **Minnesota Lawyers Encrypted Wi-Fi Account is Hacked —** Angry at a Minnesota attorney, a neighbor hacked his encrypted Wi-Fi account and e-mailed pornography labeled as family photos to his colleagues at a Minneapolis law firm, seeking to make trouble for him. The hacker also sent threatening e-mails purportedly from the attorney to the Minnesota governor and Vice President Joe Biden, and set up a fake MySpace page in the lawyer's name.

- **Mobile Technology Mishaps —** A law firm purchased iPads for every lawyer in the firm, digitized each attorney's client files, and then placed that data on the new iPads. Sometime later, there was a break-in while staff and attorneys were at lunch and the iPads were all stolen. The iPads were not encrypted or password protected.

- **Backed Up but Not Secure —** A law firm regularly backed up its computer network to several external hard drives which were rotated off site. One of these external hard drives was placed in the trunk of a car for eventual transport off site. The trunk was broken into and the hard drive was stolen. Again, there was no data encryption or password protection.

- **Could Your Trust Account Be Hacked? —** There have been unconfirmed reports of hackers sending e-mails to law firm employees that launch key-log tracking devices that are able to identify the firm's bank account information if the recipient logs into the firm's financial accounts. It then transmits that information back to the hacker, who uses it to transfer funds out of the firm's account.

- **Lost and Found Launches a Virus —** A staff person at a firm was walking in from the parking lot and found a flash drive attached to a key chain. Trying to be helpful, she took the drive into the office and inserted the drive into her USB port to try and determine who the drive and keys belonged to. This initiated the unintended download of a malicious program that turned over control of her computer to someone outside of the firm.

- **Lost or Stolen Mobile Technology —** An associate attorney at an IP boutique was going through an airport security checkpoint with a firm laptop. As she gathered her belongings together, she realized that the laptop was missing. The laptop contained highly confidential client information and was not encrypted or password protected.

- **New Target for hackers —** According to Verizon's 2011 Data Breach Investigations Report, small to medium size companies have become very attractive targets for hackers. Organized crime has gradually come to view such companies as high-reward and low-risk targets, and with automated means for stealing data from afar, they can steal as much (or more) data as from larger organizations and will often remain undetected for a longer period of time. These attacks are often costly and could result in financial stress that can cripple a small or medium size company. In Symantec's 2010 SMB Information Protection Survey, companies reported that the average annual cost of cyber-attacks for small and medium organizations was $188,242. What sort of attack could your law firm face?

Each of these stories is an example of where the appropriate use of technology still resulted in a serious data breach. Several of these examples were the result of malicious acts and others were inadvertent missteps. (For additional information on types of cybercrime consider the Department of Justice Report: "Privacy, Technology and the Law" 5/10/2011.) According to the 2012 ABA Legal Technology Survey, approximately 10 percent of all law firms have experienced a data security breach of some type and all indications are that this number will continue to rise given the incredible rate of growth of cybercrime. As lawyers we have an ethical duty under Rule 1.6 to protect the confidentiality of

client information. This includes securing the information when it is in our database, when transmitting it, storing it, or otherwise viewing or using it. The real issue that must be addressed, given that these kinds of breaches are occurring, is what steps should we take to prevent a breach and what might the fallout be for any attorney or firm whose system is involved in a data breach event?

Take Appropriate Steps to Avoid a Security Breach

Most cyber-attacks against small businesses are attacks of opportunity involving easily exploitable weaknesses. To avoid this, computer security must be a priority, not an afterthought, and there is no one-step solution that will fix the problem. Maintaining data security is a constant effort that will involve everyone in the firm from the part-time receptionist to the most senior partner. A relationship with a good IT service provider is essential to make sure the firm updates its security. Here are a few things that can be done to help secure your systems.

- Use strong pass words that include numbers, letters (upper and lower case), and symbols. Also, twelve character passwords are much harder to crack than eight.

- Password protect and encrypt data on all devices including any computers, mobile devices such as laptops, jump drives, computer tablets, external hard drives, and smart phones. If you don't know how to do this, seek help from your service provider or IT support person.

- Make sure your smart phone can be remotely wiped if lost or stolen.

- Establish a patch management system to ensure that all devices, software programs, computers, and operating systems remain current on security patches.

- Establish an ongoing training program for all staff and attorneys to safeguard against insider negligence. The goal is to ensure that no one does something like transfers work to a remote device or location such as a home computer in an insecure manner, improperly disposes of a device that is being replaced, or is tricked into opening an e-mail that was carrying a malicious payload. You might focus on keeping everyone apprised of the latest methodology being used with social engineering attacks.

- Install an Internet security software suite on all devices that will connect to the Internet. Firewalls to control access and lock out hackers are essential.

- Backup all systems and maintain a secure and encrypted copy of the backup at a remote location at all times.

- Establish a protocol for the secure use of Wi-Fi services that prohibits of the use of open unsecured public Wi-Fi-networks.

- Upgrade operating systems and Internet browsers as newer versions come to market. These upgrades often include improved security features or programing.

- To read more on law firm security see the article "The Deplorable State of Law Firm Information Security: Preventing Law Firm Data Breaches" by Sharon Nelson and John Simek.

What if If a Breach Occurs?

If your firm suspects a breach the first step is to conduct an internal forensic investigation to identify exactly which records have been exposed, and how. (For additional information on breach response see "What to Do If You Have a Security Breach in Your Data Center - The Data Center Journal" and "Data Breach Response Guide.") If a breach of information is confirmed, then appropriate authorities and affected clients should to be notified pursuant to both the ethics rules and federal and state breach notification statutes. Forty-six states and three territories (Washington DC, Puerto Rico, and the U.S.Virgin Island) have enacted laws that require those who maintain "personal identifiable information" of others to not only protect that information but to notify the owners of the information if and when a data breach occurs. (The states that have yet to enact such a law are Alabama, Kentucky, New Mexico, and South Dakota.) Virginia has enacted breach notification statutes that can be found at Va. Code § 18.2-186.6, and § 32.1-127.1:05 (HIPPA) If you maintain (un-redacted) social security numbers, driver identification numbers, credit card, or financial account information of employees or clients, these laws apply. In the event of a breach, these statutes require that state governments and those affected (for example clients or employees) by the breach be timely notified. These notice requirements are not based on where the holder of the information is located but based on where those impacted reside. Thus, a breach could result in an obligation to notify multiple state governments and comply with their various statutes.

Notification includes determining which federal or state laws apply, (current notification laws by state can be checked at the National Conference of State Legislatures, NCSL), meeting notification deadlines that can be as short as five days, setting up the contact database, verifying contact information, writing the notification letter, printing and mailing these letters, dealing with the returned mail, and handling all the calls that will come in once these letters are received. Costs for notification services alone typically run between $1 and $4 per notice. If a firm's entire contact database was breached the total cost of complying with breach notification laws could be significant. When a

breach occurs, the business or firm will frequently offer to provide credit monitoring or other types of cyber-monitoring services depending upon what type of information was breached. This can help prevent future damages to clients by protecting against identity theft and other illicit use of stolen personal information.

Managing Cyber Liability Risks

Clearly, technology is a double-edged sword. While its use by attorneys is necessary, doing so exposes attorneys to additional liabilities that can arise from identity theft, hacker malfeasance, cyber extortion, a security failure, and hardware theft. The costs of investigating and responding to these losses, and the resulting lawsuits and regulatory fines, can be staggering. The Ponemon Institute has estimated that response costs can be as high as $194 for each compromised record. Total costs for a wide breach can quickly escalate to hundreds of thousands of dollars. Many firms and attorneys have no insurance coverage to address the loss. Other damages can include damage to reputation and client relationships. Malpractice policies and most general business insurance policies offer little to no coverage for cybercrime loses. However, the risk of incurring such losses can be properly covered by the purchase of cyber liability insurance, which is becoming more widely available to small business and law firms. The carrier can also provide forensic expert advice, action plans, and notification letters and procedures to meet federal and state notification requirements. For a more detailed description of the types of coverage a cyber-policy can provide see the box to the right.

What Does Cyber Liability Insurance Cover?

Cyber liability insurance products vary greatly in terms of cost and offered coverage provisions. They are also claims-made policies, which means that they must remain in force if one is to have coverage. Policies are typically written to provide both first party coverage and third party coverage. As a group these policies are designed to provide protection against things like the following:

Conduit Injury — a lawsuit resulting from a network security failure that caused additional damage to a client's computer network

Reputational Injury — a lawsuit resulting from an attorney's participation in social media

Disclosure Injury — a lawsuit resulting from the unauthorized access to or dissemination of client information

Content Injury — a lawsuit alleging intellectual property or copyright infringement perhaps due to postings on the firm's website or blog

Privacy Notification Expenses — the costs associated with complying with relevant breach notification laws and with some policies can include the cost of attorney fees or credit-monitoring services

Crisis Management Expenses — the costs associated with bringing in outside experts to investigate the incident and fix the problem and with some policies can include the cost of a public relations consultant

Extortion Expenses — the costs associated with investigations or paying for the return of or gaining back access to data.

Consult a knowledgeable insurance broker to make sure you are getting a good product and understand the coverage's.

Addressing Your Cyber Risks:

- Identify and understand the risks
- Educate your staff
- Work regularly with a knowledgeable IT consultant to control risks
- Be aware of your ethical and statutory responsibilities
- Create a data breach response plan
- If a breach is suspected investigate and respond immediately
- Consider purchasing cyber coverage

Wendy Inge is the Virginia risk manager for Liability ALPS, the Virginia State Bar-endorsed legal liability insurer. She is available to answer risk management questions at no charge for all members of the VSB. She can be reached at (800) 367-2577.