CNA PROfessional COUNSEL℠ Advice and Insight into the Practice of Law

Protect Your Firm Against Data Security Breaches

An increasing number of law firms have experienced data security breaches. Consider the following examples and ask whether your firm may be vulnerable to similar scenarios:

- A hacker breaks into a firm's electronic files, exposing clients' confidential or personal information.
- A disgruntled employee of a firm steals clients' financial data, including social security and credit card numbers.
- A burglar breaks into a firm's office and steals its computers and backup drives.
- An employee loses a laptop computer or flash drive containing clients' confidential or personal information.
- An employee surfs unprotected websites and gets spyware infections, or uses personal webmail accounts and opens unsecured attachments.

These are not hypothetical scenarios; they are actual incidents of data security breaches that occurred at different types of businesses, including law firms. The following are some of the reported incidents collected by the Privacy Rights Clearinghouse.[1]

> In September 2006, a laptop was stolen from the trunk of the car of a law firm's auditor, containing confidential employee pension plan information -- names, Social Security Numbers, remaining balances, 401(k) and profit-sharing information for 500 current and former employees.
>
> In July 2008, Sheriff's deputies uncovered hundreds of people's personal financial files held by a law firm that had been discarded in a dumpster in northwest Houston. Box after box of records including personal financial records, documents with Social Security Numbers, people's medical files and more were found in the dumpster.

[1] "Chronology of Data Breaches," available for viewing at http://www.privacyrights.org/ar/ChronDataBreaches.htm#2008

This article offers strategies designed to mitigate the threat of data breaches and reduce potential liability for data-related losses through contractual risk transfer and insurance. It also includes guidelines that can help you mitigate damages and comply with legal disclosure and notification requirements in the event confidential information is compromised.

Preventive Strategies

In addition to required compliance with rules and regulations of professional conduct on maintaining client confidentiality, lawyers are required to comply with federal and state privacy laws. A data security breach can have devastating consequences for law firms. Potential consequences include damage to the firm's public image and reputation, diminished client confidence, and financial costs associated with the discovery, response, and notification regarding a breach, lost employee productivity, costs for credit monitoring, regulatory fines, restitution, legal fees, and additional security and audit requirements.[2]

To reduce the likelihood of such an occurrence, consider incorporating the following basic strategies into your data security program:

- Utilize an encryption system. Password protection of your firm's computers is necessary, but not sufficient, to secure firm and clients' privacy. Confidential data should be encrypted (i.e., readable only to those with the proper electronic "key") particularly when transmitted electronically outside the firm, such as through an open email system. Some jurisdictions have instituted or are considering amendments to lawyer practice rules and regulations to require encryption of lawyer/client communications, so it is important to stay abreast of developments in your jurisdiction and those in which your clients may receive your communications. Under many breach notification laws, the theft or loss of encrypted data does not trigger the duty to notify

[2] "Calculating The Cost Of A Security Breach," (June 30, 2007) by Khalid Kark with Paul Stamp, Jonathan Penn, and Alissa Dill. See CTO Forum article about the research available at http://www.thectoforum.com/article.php?prodid=664

while the loss of password protected but unencrypted information does require notification.

- Place controls on data storage and access. Clear, auditable and enforceable policies controlling access to your information system should be implemented to protect resources and data from misuse by insiders, including employees, independent contractors, vendors and customers. Frequent updates and upgrades of firewalls and anti-virus systems can prevent unauthorized access to or corruption of data by outsiders.

- Regulate use of portable devices and storage media. Formal written procedures governing the use, transport and storage of laptops, disks, flash drives, and other portable equipment should be established and enforced. Users should be reminded that portable computers are prime targets for thieves, and that the convenience of downloading client data to a laptop computer must be balanced against the possibility of loss or theft. Avoid downloading client information to a laptop computer hard drive or portable flash drive unless employees cannot access the information -- from the firm's shared drive, e.g. -- while performing out-of-office legal work for that client. Even more important is the need to delete client data from these devices once it is no longer needed to work remotely. Appropriate sanitization techniques should also be utilized when disposing of equipment or media.[3] Most releases of sensitive data have resulted from the failure to transfer this data to network systems and delete it from portable devices.

- Carefully dispose of old equipment and outdated records. Establish a record retention and destruction policy to ensure that records are retained only for as long as deemed necessary. Purge digital records in accordance with the policy, and document the destruction. An effective means of addressing the data-exposure risk associated with

[3] Sanitization is the process of removing information from media in a way which leaves no residual traces. It is commonly believed that erasing a file makes the data irretrievable. In many cases, erasing a file simply removes the pointer to that file. Data is not "deleted" unless it "wiped" using a FIPS, NIST or DOD standard compliant data erasure such as Procude or a degauuser.

obsolete computers and storage media is to "scrub" old equipment of all contents before disposing of it. Appropriate sanitization methods, such as overwriting and degaussing, should be used to remove information from storage media.[4]

- Keep a backup set of records off-site. By retaining an extra set of active records at a separate location or in secure online storage, you can help prevent large-scale data loss or corruption from a computer virus or other system breach. Electronic data should be backed up frequently, and systems should be instituted to back up the data daily and automatically.

- Communicate privacy and security policies. A sound internal communication strategy on the protection and proper use of client information featuring regular, comprehensive updates can help mitigate the risk of lost or stolen data.

Risk Transfer and Insurance

An estimated 30 to 40 percent of all data confidentiality violations involve contracted third parties, including information technology consultants and other service providers.[5] For this reason, contractual risk transfer constitutes a key element of any data security program. Whenever you entrust sensitive or non-public personal information to a third party (i.e., storage of closed client files and data), in addition to ensuring that the third party is insured, you should require signed acknowledgment of the following contractual protections:

- An agreement regarding access to and appropriate use of your information and networks, including compliance with your firm's information security standards.

[4] Overwriting is an effective method for clearing data from magnetic media. This method uses a program to write 1s, 0s, or a combination onto the media. Overwriting should not be confused with merely deleting the pointer to a file. Degaussing is a method which utilizes strong permanent magnets or electric degaussers to magnetically erase data from magnetic media. Destruction of the media is typically accomplished by shredding or burning.

[5] Ponemon Institute, "2007 Annual Study: Cost of a Data Breach," November 2007, p. 6.

- Indemnification/hold harmless agreements for all costs arising from breaches of the third party's network or the wrongful use of confidential data by their employees, contractors, agents, or other associates.

Such agreements should comply with the requirements set forth in federal and state privacy and safeguard rules, as well as applicable professional conduct rules in your jurisdiction. Lawyers may also be asked by healthcare provider clients to enter into "business associate agreements" as provided for under HIPAA regulations. When drafting or entering into such contracts, it is important to consult with an attorney experienced in data security breach regulations if you don't have such expertise in your own practice.

The full range of damages associated with a data security breach may not be covered by your firm's general and professional liability policies, depending upon the nature of the breach and the claims and damages arising therefrom. Specialized insurance products are becoming available to address technology-related risks. Consult with your insurance agent about closing any gaps in your coverage.

Post-breach Response

If you suspect your information system has been targeted and client information exposed, a rapid assessment and mitigation of damage is imperative, as outlined below:

- Evaluate the severity and scope of the incident. If a laptop computer or other portable device is lost or stolen, identify the data that may have been exposed, and determine whether these materials are encrypted or protected by password. Consider engaging forensic information technology experts to define the scope of the problem. In addition, if the possibility of identify theft or other criminal action is present, inform appropriate law enforcement agencies of the situation.

- **Notify appropriate law enforcement or other governmental authorities and potentially affected clients.** Most states now mandate notification of both governmental and/or legal authorities and of those whose confidential data may have been exposed. Firms that have experienced a data security breach also may be required to pay for credit monitoring services for potential victims. Some breach of data security laws require firms to warn affected persons of the risk of identity theft and fraud within a stipulated timeframe.

- **Consult with legal counsel regarding applicable notification laws and how to manage media coverage of the breach.** Consider going beyond minimal legal compliance. Notification of federal and state regulators, i.e., state attorney general, may be appropriate in some cases. Because clients expect law firms to safeguard personal and financial information, a data breach can tarnish your firm's reputation. You can begin to repair trust and reduce further losses by offering to help clients obtain credit monitoring and identity theft case management services.

In a computer-dependent world, the risks associated with client data exposure, theft or alteration cannot be taken lightly. Data breaches have become more common and costly. Establishing an effective data security program and preparing a post-incident response plan can help protect both clients and your firm from the occurrence and consequences of data security breaches.

Resources

- The Data Security Breach Disclosure Law Locator at http://www.guardianedge.com/resources/breach-disclosure.php
- FTC Federal and state laws on identity theft http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/laws.html
- The Federal Trade Commission's identity theft Web site, at http://www.ftc.gov/bcp/edu/microsites/idtheft/, contains information, tools and additional links relating to data security.
- The Privacy Rights Clearinghouse Web site, at http://www.privacyrights.org, offers a range of resources for

understanding, preventing and mitigating data security breaches, including a frequently updated "Chronology of Data Breaches."

- The web site for the Privacy and Information Security Committee of the Antitrust Law Section of the American Bar Association at http://www.abanet.org/dch/committee.cfm?com=AT311550, offers articles available to non-members and members.
- Information Security for Lawyers and Law Firms, Nelson et al, editors, American Bar Association Publication. See http://www.abanet.org/abastore/index.cfm?section=main&fm=Product.AddToCart&pid=5450043
- Law.com's Legal Technology web site at http://www.law.com/jsp/legaltechnology/security.jsp, offers regularly updated articles and information on this topic.

May 2009

CNA