

mutuallyspeaking

Cyber Crime and Law Firms



A different kind of risk is developing: cyber liability. We all have seen the news in the last several months in which the computer system for the big retailer Target was hacked, affecting some 40 million customers. Other large companies hit by security breaches include Nieman Marcus, TJX Companies, and AOL, among others. Maybe the one that hits closest to home for lawyers is the Washington State Administrative Office of the Courts. In that data breach, names, social security numbers and driver's license numbers were accessed.

McAfee, the Internet security company, released its latest comprehensive 2014 security report at the end of December. It raises the question about how well prepared we are for what could be coming in 2014.

Mobile devices have become even bigger targets. The report concludes that attacks will increase in 2014. Such attacks grew a whopping 33 percent in 2013, while PC attacks were flat, showing that malware creators have largely shifted to more-vulnerable mobile operating systems.

As a lawyer, you always had an

obligation to keep client information confidential. But now, in addition to more information being stored electronically than ever before, two changes have increased that obligation. The first is that storage of client information is much more portable, e.g., laptops and smartphones; and the second is a statutory obligation to protect Personally Identifiable Information (PII) for more than just clients.

What would you do if you lost sensitive client information? Whether because of a data breach due to hackers, careless disposal of client records, theft of mobile devices or misuse of internal security protocols, lawyers need to consider how they are protecting client and employee information. Experts say law firms have become a prime target because of all the sensitive and confidential Personally Identifiable Information stored in law firm databases.

The consequences of a breach or lost data can be monumental, especially for solo practitioners. Sandy Hauserman, a lawyer from Vermont who became a

Cybercrime continued on page 2

Advising Family Business Clients—Keep Claims Risks in the Back Of the Family Minivan

By Atty. Kevin J. Palmersheim
*Haley Palmersheim
Madison, Wisconsin*

Leo Tolstoy once wrote, “All happy families are alike; each unhappy family is unhappy in its own way.” With that kind of prescient observation it’s hard to believe little Leo was never in the back seat of the family Minivan, engaged in a turf battle with his siblings, while his parents were yelling, “Stop touching each other! Don’t make me turn this car around!”

Solo practitioners, small firms and general business lawyers often do hear the detailed family stories—and sometimes are smack dab in the middle of the battle—in the course of providing legal advice to family business clients. Furthermore, because each family has the potential to be unhappy in its own way, these family business clients trigger a unique set of concerns for lawyers and lawyers need to be wary of the related risks.

It is not surprising that so many business legal issues involve family



Kevin Palmersheim

Palmersheim continued on page 4



Practicing law can be fulfilling and satisfying as lawyers help people in need. However, for a variety of reasons, things can sometimes go wrong.

By Brian Anderson

Lawyer’s exposure when relying upon information provided by another professional in advising a client

Lawyers often become involved in matters for which the lawyer relies on reports or opinions of other professionals. That information is then used in developing a strategy to help the client or is the basis for the legal advice provided. Examples of these types of situations include an accountant providing tax advice for a personal or corporate transaction, an appraiser involved in a divorce, a surveyor drafting a legal description or a bank trust officer dealing with a client’s trust. A lawyer may assume that the client has been adequately advised on the important aspects of the transaction by the other professional, which may not be the case. Furthermore, a lawyer may assume that the other professional competently prepared the documentation or report, which also may not be the case.

Even though it is common for a lawyer to rely upon documentation prepared or provided by another professional when rendering legal advice to a client, it is important to recognize that there is a risk that the client may assert a claim against the lawyer if the information relied upon turns out to be inaccurate and the client sustains a loss. The client may not understand that the substantive legal advice and work that you provided was based upon the information prepared by another professional, unless you clearly inform the client of that fact. The lawyer should advise the client of his or her role at the time of the initial engagement and communicate what advice will or will not be provided, to avoid any misunderstanding. Make it clear to the client, in writing, that you are relying upon the accuracy of the information prepared by another professional. If you are not providing a title opinion, tax advice or recommending an investment strategy, make sure that the client understands that to be the case. Written documentation outlining the scope of your retention is an important safeguard to protect you in the event the information you relied upon turns out to be wrong.

If the documentation prepared by another professional is obviously wrong, a client may blame the lawyer for not bringing the problem to the client’s attention. Therefore, you should always review all of the documentation that you rely upon to best protect yourself and serve your client. If you have not been provided any or all of the important documentation that you believe is necessary to render an opinion, this should also be brought to your client’s attention as well. The failure of the lawyer to distinguish his or her role from that of other professionals involved in a client matter, in writing, is often the missing document that exposes a lawyer to a legal malpractice claim caused by the other professional’s mistake.

Finally, a lawyer may also be exposed to a claim when relying upon inaccurate information received by the client’s previous attorney or referral counsel. These types of scenarios include personal injury claims in which the statute of limitations is misidentified, an erroneously drafted QDRO or one that was never completed, or in a bankruptcy case where a client’s debt obligations or assets were not accurately identified or disclosed to the trustee. If a client is damaged and the second lawyer could have prevented the harm but failed to do so, that second lawyer is responsible for causing the damage, even though the original mistake was made by the client’s first attorney. ■



Founder and Managing Member of Digital Risk Resources (“DRE”), an insurance product development company, described to a WILMIC seminar audience late last year how cyber exposures effect law firms – what those exposures are and how he expects they will grow. “Every law firm is now dependent on technology and the internet,” he says. “This dependency creates business risk not covered in standard Errors and Omissions or Property/Casualty policies.”

Client records and credit/debit card processing make up a significant portion of the overall risk profile. Law firms gather and transmit Personally Identifiable Information (PII) of clients, employees, vendors and others. Law firms collect a lot of very sensitive information which could severely damage a client’s reputation.

Aside from the hackers with bad intent, you could lose sensitive client information very innocently. What if you mistakenly left your laptop, tablet or your smartphone at the courthouse, in an airport, or at the local coffee shop and it contained client information? Some lawyers have already experienced this.

Why is cyber risk something to which lawyers should pay attention? First, Wisconsin is one of many states that have enacted breach notice laws that require a business suffering a security breach or losing PII to notify victims so they can take action to protect themselves from identity theft. In addition, any law firm storing



medical information is subject to the notification rules of HIPAA. Notification costs can grow rapidly. Hauserman says the average cost is between \$50 and \$214 for each affected person.

WILMIC Now a Source For Cyber Liability Insurance

WILMIC now offers a cyber liability insurance policy. It includes three types of coverages:

1) Breach Notice Coverage which provides coverage for costs incurred by a lawyer or law firm to comply with Wisconsin's privacy breach notice law, as well as notice fulfillment services and credit and fraud monitoring for clients whose confidential information has been lost or stolen;

2) Privacy Liability Coverage which covers third party liability for loss of Personally Identifiable Information; and

3) Security Breach Liability Coverage which covers third party liability and damages from computer security breaches such as virus and hacker attacks if those breaches were within the law firm's information system.

If you are interested in getting more information about cyber risk coverage, call WILMIC at 800-373-3839. We can walk you through the process.

Others in the legal professional liability insurance industry have written about cyber crime. The following is reprinted with permission from LawPRO magazine and author Dan Pinnington, Vice President Claims Prevention and Stakeholder Relations at Lawyers' Professional Indemnity Company (LAWPRO®) in Toronto, Ontario, Canada. Many thanks to Dan and the LawPRO staff for allowing us to reprint this article.

Historians may well look back and call 2013 "The year of the hacker." There have been numerous high-profile data breaches involving major corporations and online services: Facebook, Apple, Twitter, Adobe, NASDAQ, The New York Times and LexisNexis, to name just a few. Everyone reading this article likely has information stored by at least one, if not several, of these companies.

And it doesn't stop there. Millions of other business entities and individuals have experienced data breaches this year, either directly on their own computers or systems, or indirectly where there was a data breach involving information about them that was stored with a third party. Countless others will have lost money after being duped in various online scams.

Law firms and lawyers take notice: cyber criminals are specifically targeting you because they want your data or the money in your trust account. Law firms are actually very appealing and sought-after targets for cyber criminals for three reasons. Firstly, law firms have large amounts of sensitive and confidential information that can be very valuable. Secondly, law firms tend to have very large sums of money in their bank accounts. Lastly, and not the least, relative to their clients and based on anecdotal information, law firms tend to have weaker security protection in place on their networks and systems.

Cyber criminals will use every tool at their disposal to attack law firms. They will send spam and phishing messages. They will try to install malware and create backdoors into your firm's computers. They will look for weaknesses in security

configurations and exploit them in order to access firm networks. In very devious ways, they will try to trick you or your staff into helping them. It is quite possible they would target you individually, including attacking your home computer to hack into your office systems.

The bottom line: cybercrime is a real and present danger for law firms. All firms should work to understand the cybercrime risks they are exposed to and take steps to reduce the likelihood they will experience a data breach at the hands of cyber criminals.

How prepared are you?

To assess your cybercrime preparedness, see if you can answer the following questions:

- Are your passwords secure enough?
- Would you or your staff be duped by a phishing message?
- How would your firm respond if one of its servers was hacked?
- Is your anti-malware software the most current version and is it updated?
- Could you tell if your computer had malware on it?
- Are your computer's security settings adequate?
- Is there a backdoor into your network?
- What would happen if a firm laptop or smartphone were lost or stolen?
- How would you deal with a major data theft by an ex-employee?
- Is your home computer safe?

Cybercrime dangers are many, complex and ever-changing. Hardly a day goes by without another news report of a data breach or other cyber-related scam or theft. Cyber criminals have considerable resources and expertise, and can cause significant damage to their targets. Cyber criminals specifically target law firms as law firms regularly have funds in their trust accounts and client data that is often very valuable.

The cybercrime dangers firms need to address are many and varied:

1. Avoid the dangers of email
2. Lock down your browser and avoid surfing dangers

3. Avoid infections with antivirus and/or anti-malware software
4. Lock things up by using passwords properly
5. Address security vulnerabilities by installing operating system and program updates
6. Keep the bad guys out with a firewall on your Internet connection
7. Stump hackers by changing key default settings
8. Lock down and protect your data wherever it is
9. Scrub confidential client information on discarded equipment
10. Be safe when using remote access and public computers
11. Secure your mobile devices to protect the data on them
12. Harden your wireless and Bluetooth connections and use public Wi-Fi with extreme caution
13. Be careful about putting your firm's data in the cloud
14. Inside people can be the most dangerous
15. Be careful of the dangers of BYOD and family computers
16. A backup could save your practice after a cybercrime incident

As they can be used as a point of access to your firm's systems, it is critical to address the above issues on your personal smartphones and tablets, as well as your home computers and networks. You must address all the dangers. Don't be tempted to ignore any of the dangers listed above, or to skip or skimp on the steps suggested to deal with them. Remember, your data and systems are only as safe as the weakest link in your security plan. When you leave on vacation, you lock every door and window in your house. Leaving just one door or window open gives a thief easy and instant access. To protect yourself from cybercrime, it is critical that you fully and properly address all cybercrime dangers. Cyber criminals will look for and exploit holes in your security plan. ■

—Dan Pinnington

Palmerseim continued from page 1

businesses. Ninety percent of U.S. businesses are controlled by families. Family businesses also account for about 50% of the gross domestic product in the U.S., and create about 60% of the jobs (not including jobs like mowing the lawn or cleaning out the garage, which I contend my parents unfairly made me do far more often than my younger brothers).

Attorneys face greater risks in advising family businesses for various reasons, most of which fall into the following categories:

It is often easier and preferable to pin the blame on the attorney who is an integral advisor, rather than other family members.

1. It is often easier and preferable to pin the blame on the attorney who is an integral advisor, rather than other family members. The blame factor is related to a couple factors. Not surprisingly, family members will be reluctant to accept personal responsibility for bad decisions or business failures, and may use the business lawyer as a convenient scapegoat. Furthermore, when a lawyer identifies one family member being responsible for hurting the business the other competent family members may remain reluctant to single out their kin – kind of like the philosophy that “no one picks on my brother but me.”

2. If the lawyer is associated with a family member who is being blamed or sued, then that lawyer is also a target to be sued. When a lawyer represents a family business, he or she frequently ends up working more closely with some family members than others. This may be because of the family member's position in senior management, or simply because some people are more predisposed to talk to the company attorney than others. The risk is that the lawyer is perceived to be

more closely aligned with those family members with which there is the most contact. If there is a falling out among the family the attorney will end up being linked with one group and may get sued by the other family members.

3. The statute of limitations is longer for claims against outside advisors, like lawyers, than it is for alleged wrongdoers within the business. The statute of limitations for professional negligence is six years. Meanwhile, the statute of limitations for breach of fiduciary duty and other intentional torts by insiders is usually no more than three

years. By the time a disgruntled business owner gets around to suing the limitation may be expired for the alleged wrongs committed by the business insiders, but not for the lawyer who was advising the business and possibly the insiders.

4. The economy is struggling. Blood may be thicker than water, but the reason lawyers get sued is often related to the perception that the lawyer's wallet is thicker than the business owner's. A bad economy, coupled with a failed or severely injured family business, makes the lawyer an attractive target. Furthermore, in a tight economy people generally fight over smaller sums of money and pursue weaker claims than they would when times are good.

Lawyers can minimize their risks with advising family businesses, and many of these guidelines work just as well to limit risks with clients in general.

A Be clear on the identity of your client, and confirm that in writing. When hired by a family member regarding issues with a family business, be clear about whether you represent that family member, a group of family members, or

the business itself. Confirm your representation in writing—preferably in an engagement letter or fee agreement.

B. When you take on more business, be aware of potential conflicts of interest and obtain written waivers. When a lawyer is retained by family business owners,

One overriding principle when representing family businesses is to frequently communicate with the client(s), both verbally and in writing, and try to assist the family in derailing any potential problems before they become big problems.

it is quite common for that representation to expand into other legal matters. Building an ongoing client relationship is one of the satisfying aspects of practicing law and advising businesses. When working on collateral matters, however, the lawyer needs to be wary of potential conflicts of interest among family members and the business. If the potential conflict is waivable, then the attorney needs to obtain informed consent from the clients by having them sign a written waiver.

C. Identify your contact person in the business, but keep in touch with other owners. To avoid getting linked to one family member or group, the lawyer should try to communicate from time to time with all the family owners. This can be as simple as copying them on correspondence or on the renewal of their annual registration statement with the Wisconsin Department of Financial Institutions.

D. Strongly advise clients to adopt buy-sell agreements and draft comprehensive buyout provisions. I identified earlier in this article how lawyers may be sued if there are disagreements among family members. One way for the lawyer to protect him or herself is to first protect the business and family by drafting binding ownership agreements. These agreements should always include provisions that allow for a disgruntled family member to leave the business. The buy-sell should also have

a mechanism for the ownership interest to be sold and purchased under certain circumstances, and to make the triggering mandatory for both sides (for example, in the event of death, disability, termination of employment, or voluntary withdrawal from the business). Clients will often tell the law-

yer that they don't want mandatory buy/sell provisions and that the family will "work out" any future issues when they arise. In those circumstances, I usually reply by asking whether the business owner knows of anyone who has divorced a spouse, and remind the owner that married couples also expect everything to work out and yet there is frequently a subsequent split. I further explain that the costs of drafting a buy-sell agreement are a fraction of the costs of litigating a business break-up.

One overriding principle when representing family businesses is to frequently communicate with the client(s), both verbally and in writing, and try to assist the family in derailing any potential problems before they become big problems. Of course, regardless of a lawyer's diligence and advice the nuances of family businesses occasionally mean that problems cannot be avoided. This happens more often in family businesses because of the personal baggage and philosophies that family members bring with them—for example, my mother's conviction that most of the world's problems could be solved if only her grandsons would get a haircut.

By applying a little planning and being aware, lawyers can reduce their risks of a professional negligence claim and, more importantly, foster a long-term relationship with a good family business client. Personally, I prefer that outcome to a long car ride with my brothers invading my personal space and touching me—for the record, I just want to make clear that they started it! ■

WILMIC Once Again Part of This Year's Young Lawyers Division Leadership Conference

For the third consecutive year, Wisconsin Lawyers Mutual Insurance Company is providing support to the State Bar's Young Lawyers Division. The YLD's annual Leadership Conference is scheduled for Friday, March 21 at the Tundra Lodge in Green Bay.

In addition to providing a sponsorship for the conference, WILMIC is also co-presenting a CLE program titled, "Ten Risk Management Tips For Young Lawyers." The program will discuss malpractice risks and ethics rules young lawyers should consider when looking for a legal job, establishing a legal practice and trying to find clients. WILMIC Senior Vice President Tom Watson and Tim Pierce, Ethics Counsel with the State Bar of Wisconsin, will be presenting the program. ■

mutuallyspeaking

WINTER 2014

CONTACT US

608-824-1700

608-824-1701 fax

800-373-3839

wilmic.com

Office hours at Wisconsin Lawyers Mutual Insurance Company are 8 am until 4:30 pm Monday–Friday. Other information also found at wilmic.com.

Wisconsin Lawyers Mutual
INSURANCE COMPANY



725 Heartland Trail, Suite 300
Madison, WI 53717

Presort Std.
U.S. Postage
PAID
Madison, WI
Permit No. 1949

WILMIC Agency a Good Source for Court Bonds

WILMIC's bond agency is in its second year of operation and many lawyers who have taken advantage of the service have found very competitive prices. Any Wisconsin lawyer who needs a bond can turn to the Wisconsin Lawyers Insurance Agency, a subsidiary of WILMIC.

Through the agency, lawyers are directed to The Bar Plan of Missouri, which offers attorney-managed underwriting and provides the bonds at a very competitive cost. The Missouri company handles all processing and claims as well.

Bonds available to Wisconsin lawyers include:

- Fiduciary Bonds (Administrator, Executor, Conservator, Estate)
- Court Bonds (Appeal, Replevin, Injunction, etc.)
- Notary Bonds
- License and Permit Bonds
- Lost Instrument Bonds
- Public Official Bonds
- ERISA Bonds

The Missouri company has a 24-hour turnaround policy after obtaining all necessary information and resolving any questions with applicants. For access to the online application process, go to WILMIC's website, www.wilmic.com and click on "Apply For Court Bonds." To apply by telephone, call 1-877-553-6376. ■