VOLUME 28, ISSUE 1 WINTER 2016

THE RISK MANAGER

A QUARTERLY NEWSLETTER BY LAWYERS MUTUAL INSURANCE COMPANY OF KENTUCKY

Cyber Security Special Edition

KENTUCKY LAWYERS AND CYBER SECURITY RISK MANAGEMENT

IN THIS ISSUE *of the newsletter Lawyers Mutual inaugurates its coverage of the growing impact of technology on the delivery of legal services and the risks this creates for client confidentiality and damage to the firm. Law firm cyber security risk management requirements have changed what it means to be a competent lawyer. In addition to law and procedure lawyers now have a new duty to be technically competent about the devices they employ in their practice. This duty extends to use of all technology, including computers, mobile devices, networks, technology outsourcing, and cloud computing. Lawyers who lack the technical competence to provide cyber security for devices that contain confidential information risk bar disciplinary action and malpractice claims. Fundamental knowledge of cyber security is now an essential lawyer competency.*

In this special issue we offer four articles covering lawyer's liability for data breaches, risk management guidance for defending your firm from hackers and scammers with special emphasis on cloud computing, and how to advise a board of directors on cyber security in either the capacity of board member or legal advisor to the board. Future newsletters will bring you cyber security developments to assist you in maintaining your technical competency.

DON'T MISS

"CYBER LIABILITY ISSUES FOR ATTORNEYS"

FRIDAY, MAY 13, 2016
9:00 A.M.
2016 KBA CONVENTION

This program, in the format of a panel discussion, will explore in detail cyber security issues and essential lawyer competency requirements.

ATTORNEY'S LIABILITY FOR DATA BREACHES[1]

RUTH H. BAXTER
Crawford & Baxter, P.S.C.
President, Lawyers Mutual Insurance Company of Kentucky

Beginning in 2009, state and federal law enforcement agencies have warned larger United States law firms that their computer files are targets for cyber spies and thieves looking for valuable information about potential corporate mergers, patent and trademark secrets, litigation plans, and financial data of corporate clients. A trade dispute for a maker of solar panels recently subjected a Washington, D.C. law firm to Chinese military hackers. A client's computer breach resulted in a hack of a New York law firm that infiltrated not only its client base, but also resulted in the loss of its own employees' social security numbers. "If you are a major law firm, it's safe to say that you've either already been a victim, currently are a victim, or will be a victim..."[2]

Solo practitioners and smaller law firms should not think they are immune to cyber attacks. As a partner in a three-attorney law firm reported last year, his firm was a victim of a new Cryptolocker-type virus, a ransomware used to encrypt his client files so they were unreadable. The hackers demanded money to restore the data. "Dear Clients", Attorney Robert Ziprick wrote in the letter the law firm mailed out giving notice to its clients, "It is almost a daily occurrence that we read about

CONTINUED ON PAGE 2

INSIDE THIS ISSUE:

Lawyers Mutual
www.lmick.com
MEMBER NATIONAL ASSOCIATION OF BAR RELATED INSURANCE COMPANIES

DATA BREACHES

CONTINUED FROM FRONT PAGE

cyber attacks in the news. Unfortunately, our firm was the victim of a single cyber attack...."[3] The point is that all law firms are at a higher risk for cyber-intrusions than ever before. Attorneys must assess how their vulnerability to third party attacks can make them liable for failing to protect client information.

This article is intended to provide an overview of what these developments mean to Kentucky lawyers and offer cyber security risk management considerations to assist you in protecting your firm from professional responsibility violations and malpractice claims.

KENTUCKY'S CONSUMER PROTECTION DATA BREACH NOTIFICATION LAW KRS 365.732

The Kentucky General Assembly joined 40 other states when it enacted a consumer protection data breach notification law in 2014. KRS 365.732 requires written notice to persons affected by a computer security 'breach' involving their unencrypted 'personally identifiable information.' Breach is defined as the unauthorized acquisition of unencrypted and unredacted computerized data that can compromise the security and confidentiality of an individual.[4] An individual's first name or first initial, in combination with a social security number, driver's license number or an account number or credit card with the required password, constitutes personally identifiable information under the statute. The 'information holder,' in our case the attorney, is required to disclose any breach to the client, in an 'expedient time' and 'without reasonable delay.' The only exception for not notifying clients quickly is if there is a pending criminal investigation by a law enforcement agency.

The notification required under the statute is to be in written form, or, may be sent electronically if the client has agreed to accept such notices.[5] If the cost of providing individual notices exceeds $250,000, or the class of persons affected exceeds 500,000 people, then a 'substitute notice' by email posted on the information holder's website, coupled with statewide media notification suffices. If more than 1,000 persons are impacted at any one time, the statute mandates that the information holder notify all consumer reporting agencies and credit bureaus that maintain consumer files on a nation wide basis. The timing, distribution and content of those notices are prescribed by federal law.[6]

The data breach notification statute establishes no new cause of action. Nor does it authorize fines or penalties for

CONTINUED ON PAGE 3

"TECHNOLOGY EVOLVES SO MUCH FASTER THAN WISDOM." *Jennifer Stone*

DATA BREACHES

Continued from page 2

non-compliance. However, KRS 446.070 allows a person injured by the violation of any Kentucky statute to recover damages sustained by reason of the violation.

The greatest harm inflicted to a law firm by a data breach is the violation of the attorney's duty to keep and preserve a client's confidential information.[7] However, from the business aspect of the law firm, reputational damage and loss of client confidence can have a significant impact on the firm's bottom line. Thus, cyber security oversight and management for law practices is essential.

DATA BREACH CYBER SECURITY RISK MANAGEMENT

Cyber Security Assessment and Plan: Efforts to protect your law firm from data breaches begin with a law firm discussion on cyber security issues and the development of a plan to detect intrusions, respond to those intrusions, and mitigate their impact with an effective response. Discussion should first focus on an assessment of all cyber security risks associated with the law firm's use of technology, including email communications, e-filings with state and federal courts, the exchange of discovery in litigation, and maintenance and storage of digital client information and files. *Have you appropriately assessed all of your law firm's cyber security risks? What steps have been taken to evaluate those risks?*

1. In the event of a breach, does your law firm have an effective response plan?
2. Who is responsible for the implementation of the plan?
3. Are employees of the law firm aware of the plan and trained in the role they play?
4. Has the plan been tested to make sure it works?
5. How are communications with clients, the court, and third parties to be handled?
6. Do you have the resources to make the notifications required by Kentucky law to your clients?

Evaluate Your Law Firm's Computer Practices:

1. Do you have a written computer and information system policies and procedures?
2. Do you require employees to follow those policies and procedures?
3. Do you use commercially available firewall protection?
4. Do you use commercially available anti-virus protection?
5. Do you install updates to those protections in a timely manner?
6. Do you have alternative controls to prevent unauthorized access or intrusion to your systems?
7. Do you have and enforce policies concerning the encryption of internal and external communications?
8. How is the use of portable computers or portable media devices affected by these policies?

Consider Your Law Firm's Operational Practices:

1. How are passwords established, recorded, and updated?
2. When an employee leaves do you terminate all computer access and user accounts, change pass codes and use authorizations?
3. When you obtain a client or a third party vendor, do you verify security information and privacy controls and then monitor or audit them?
4. When you terminate a client or a third party vendor, do you terminate its computer access and user accounts, as well as email authorization?
5. What format do you utilize for backing up and storing computer system data?
6. Do you have the competency to evaluate your IT system or is a third party the appropriate entity to make that evaluation?

CYBER SECURITY LIABILITY INSURANCE

Cyber security liability insurance emerged at the end of the 1990's to cover losses of revenue and data restoration costs from corporation cyber attacks. It was not until California passed the world's first data breach notification law that demand for commercial coverage for law firms began. Insurers now provide cyber security liability insurance coverage to pay for expenses associated with notification to clients, credit monitoring for the affected clients, IT forensics, public relations fees, defense costs and civil fines from privacy regulation actions, and civil litigation. Some policies also extend coverage to address loss of income as a consequence

CONTINUED ON PAGE 11

"IF YOU DON'T KNOW HOW TO DO SOMETHING, YOU DON'T KNOW HOW TO DO IT ON A COMPUTER." *Jerry Leichter*

ETHICS STILL APPLY: EVEN WHEN YOUR HEAD IS IN THE 'CLOUD'

JAKE A. THOMPSON[1]
Crawford & Baxter, P.S.C.

INTRODUCTION

As all Kentucky attorneys are aware, the Kentucky Supreme Court Rules of Professional Conduct (*SCR 3.130*) impose many professional obligations on attorneys in their handling and safekeeping of client information and property. When client files, communications, documents, or other client data are stored in digital form, it becomes subject to the risks of a cyber attack. Attorneys must be aware of these risks and ensure compliance with their ethical obligations when managing them.

One technological advancement that holds appeal for many attorneys, and also implicates many ethical considerations, is 'cloud-computing.' Cloud-computing is processing power, storage space, software, or other computing services, often accessed via a web browser.[2] As one state bar association pointed out, the term cloud-computing includes the use of smartphones; iPhones; web-based email such as Gmail, Yahoo, Hotmail, or AOL Mail; and products such as Google Docs, Microsoft Office 365, or Dropbox, along with many others.[3]

Some of these services are email services. Others provide solely for the storage of documents in the cloud on servers owned by third party server-providers. These servers can be located in a distant warehouse, out of state, or out of country. They are accessible only on the Internet. Some are complete cloud-based programs in which the software is not installed on the user's computer, but is accessed on the Internet. Younger attorneys learned to rely heavily on cloud-computing in law school. They realize the value of cloud-computing and use some form of it every day. As useful as cloud-computing is, it introduces significant new ethical considerations for attorneys because client data is no longer in the sole possession of the attorney.

This article addresses the cyber security risks and professional responsibility duties this technology raises and offers risk management considerations in avoiding malpractice claims and bar complaints for failing to competently use technology in your practice.

CLOUD COMPUTING IN KENTUCKY

The KBA in Ethics Opinion *KBA E-437* (3/21/14) approved the use of the cloud by Kentucky lawyers as follows:

A lawyer may use cloud-based services with regard to confidential client information. In using cloud-based services, a lawyer must use reasonable care to assure that client confidentiality is protected and client property is safeguarded. See *SCR 3.130(1.6(a))* & *(1.15(a))*.

A lawyer must act consistent with his or her duty of competence in selecting and monitoring the providers of cloud-based services. See *SCR 3.130(1.1)*. A lawyer must use "reasonable efforts" to ensure that the conduct of providers of cloud-based services assisting him or her is compatible with ethical obligations of the lawyer, and, if the lawyer is a partner or otherwise has managerial authority in a law firm, the lawyer must use "reasonable efforts" to make sure that the firm has measures in place to assure that providers of cloud-based services engage in conduct compatible with ethical obligations of the lawyer. See *3.130(5.3(a)* & *(b))*. Finally, a lawyer must consult with the client about the use of the cloud if the matter is sufficiently sensitive such that the duty to "reasonably consult with the client about the means by which the client's objectives are to be accomplished" is implicated. See *SCR 3.130(1.4(b))*.

CONTINUED ON PAGE 5

"IN SOFTWARE SYSTEMS, IT IS OFTEN THE EARLY BIRD THAT MAKES THE WORM" — *Yale University: Epigrams in Programming*

ETHICS STILL APPLY

CONTINUED FROM PAGE 4

The opinion offered this guidance in meeting professional responsibility requirements:

> Just as a lawyer should review the terms of storage for a warehouse for storage of client files, so too should a lawyer review the terms of the arrangement regarding online storage or treatment of confidential client information or other cloud-based service. Some questions that a lawyer should consider in this regard include the following:

- What protections does the provider have to prevent disclosure of confidential client information?
- Is the provider contractually obligated to protect the security and confidentiality of information stored with it?
- Does the service agreement state that the provider "owns" the data stored by the provider?
- What procedures, including notice procedures to the lawyer, does the provider use when responding to governmental or judicial attempts to obtain confidential client information?
- At the conclusion of the relationship between the lawyer or law firm and the provider, will the provider return all information to the lawyer or law firm?
- Does the provider keep copies of the confidential client information after the relationship is concluded or the lawyer or law firm has removed particular client information from the provider?
- What are the provider's policies and procedures regarding emergency situations such as natural disasters and power interruption?
- Where, geographically, is the server used by the provider for long-term or short-term storage or other service located? (*footnote omitted*)

A REVIEW OF APPLICABLE KENTUCKY RULES OF PROFESSIONAL CONDUCT

A. First, an attorney must act competently and reasonably in handling and storing client data. *SCR 3.130 (1.1)* of the Kentucky Rules of Professional Conduct requires attorneys to provide competent representation, and to utilize the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation. Kentucky has not adopted the ABA's changes to Model Rule 1.1 that, in comment (8), advises that for an attorney to maintain the requisite knowledge and skill, the attorney must keep abreast of the changing benefits and risks of relevant technology. The ABA made it clear that this change was not a new requirement. Rather it makes explicit what was heretofore implicit. *KBA E-437* removes any doubt that Kentucky lawyers must be competent in the use of technology in their practice.

B. *SCR 3.130 (5.3)* governs the responsibilities of attorneys for the conduct of nonlawyers employed by the attorney. The rule makes it clear that an attorney can be held responsible if a server-provider improperly handles client data. Attorneys cannot simply put client data into the cloud and blindly trust that the server-provider will protect the data. Attorneys need to investigate the server-provider to ensure the provider is reputable.

C. *SCR 3.130(1.6)* requires attorneys to protect the confidentiality of client data. An attorney cannot simply put client data into the cloud, and assume it will remain confidential. The storage of data in the cloud is like storing client files in an offsite warehouse. In such a case, the attorney will review the contract with the warehouse to ensure there are enforceable requirements that the warehouse keep files secure, prevent third parties from accessing the files, and that the employees of the warehouse protect the confidentiality of the files.

The same obligations and considerations apply to online storage. Attorneys must:

- Read the Terms of Use, Terms of Service, End User Licensing Agreement, and any other such agreement, to ensure the provider is obligated to keep the data confidential.
- Ensure that agreements do not grant the server provider proprietary interest in the data stored on its server.
- Be aware of how a server-provider will respond to subpoenas, warrants, civil search and seizure actions, or other third party requests for information to ensure client data is not improperly disclosed.
- Be aware that data stored in the cloud is not really stored in the air, but is actually stored on a physical server that the attorney is accessing remotely on the Internet. The server may be located in a different country or in a different state.

CONTINUED ON PAGE 6

"IF A LISTENER **NODS HIS HEAD** WHEN YOU'RE EXPLAINING YOUR PROGRAM, **WAKE HIM UP.**" *Yale University: Epigrams in Programming*

ETHICS STILL APPLY

CONTINUED FROM PAGE 5

- Be knowledgeable of the laws in the jurisdiction in which the server is located to ensure that the data is as protected by the law in that jurisdiction as it would be in Kentucky.
- Be aware of any potential waiver of the attorney/client privilege.[4] Waiver issues may arise when emails and attachments are sent to a client using her employer's email server, especially if the employer is involved in the litigation. Waiver issues may also arise in other case-specific circumstances when a cloud-computing provider is involved in the dispute.

D. *SCR 3.130 (1.15)* governs the safekeeping of client property that includes client data. To comply with this rule attorneys should:

- Investigate the security measures taken by the server-provider to ensure the client data is kept safe and reasonably protected from theft and cyber attacks.
- Consider having an express agreement with the server provider to keep information confidential and secure.[5]
- Determine whether access to the data is sufficiently password protected, and whether the data is encrypted. The attorney is ultimately responsible for the protection and safekeeping of the client's data.
- Consider using electronic audit trail procedures to monitor who is remotely accessing the stored data.[6] This allows an attorney to continually monitor who is accessing the data to ensure an unauthorized device is not accessing the data.

OTHER CONSIDERATIONS

A. Continued Access: In addition to keeping client property safe, attorneys must ensure continued access to client data. To accomplish this attorneys should:

- Be sure that the service-provider does not destroy documents before the applicable retention period expires.
- Be aware of and consider the potential for server outages and technical issues that could prevent accessing documents or information.
- Consider the actions to be taken if the service-provider goes out of business, is bought out or merges with another company, enters bankruptcy, or otherwise suffers a break in continuity.
- Be aware of what will happen to documents in the cloud should the attorney fail to pay applicable subscription fees.[7]

B. What Files Should Go on the Cloud? While retention and access are concerns whether the files stored in the cloud are backups or the primary client files, special concern should be given to any client data that does not have a backup outside of the cloud. It is noteworthy that when many state bar associations issued specific opinions on storing client files in the cloud, they framed the question as whether it was proper to use the cloud *as a backup*.[8]

Whether it is reasonable to maintain the *only* complete copy of client files in the cloud, is a very different question. Prudence would caution any attorney to be wary of relying on the cloud as the only access to client data. The Alabama State Bar noted that while certain client documents could be destroyed after scanning and converted to digital format, the best practice is to follow the procedure used for ordinary paper documents.[9] The Alabama State Bar also noted that unlike traditional paper files, a lawyer must back up all electronically stored files, and approved the use of cloud storage for this purpose.[10] The easiest and best practice for Kentucky lawyers is to backup all digital client data.

C. Firing Your Server-Provider: If the attorney becomes dissatisfied with the server-provider or otherwise decides to use a different service to store the data, the attorney must be able to move the data from the server-provider to another server, whether private or in the cloud. Attorneys should investigate whether, after such a move is made, the server-provider can, and will, wipe the client data from its servers so that no data will be left with the old server. Attorneys should not merely stop using the server and leave client data on that server.

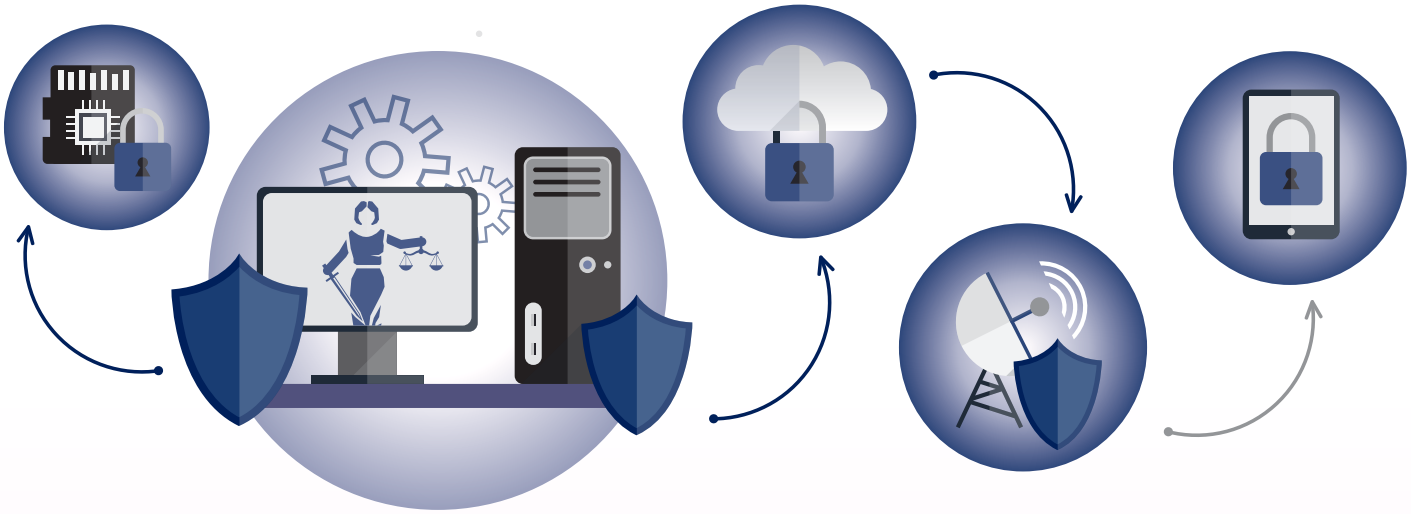
D. Special Risks of Smartphones and Tablets: Smartphones and tablets due to their cloud-connectivity pose an added risk to client data. Attorneys must be aware of whether client data stored in the cloud is easily accessed from their smartphone or tablet if it is lost or stolen.

Attorneys should ask the question: "If my smart phone or tablet is lost or stolen, how easy would it be for someone to access my client data, and how much client data would be available to them?" Documents stored in servers such as Google Drive, iCloud, and many others, can often be accessed from a smartphone without having to re-enter a password if the user

CONTINUED ON PAGE 11

"SISYPHUS WAS LUCKY! HE DIDN'T HAVE TO KEEP FIGURING OUT ALL OVER AGAIN HOW TO ROLL THE STONE FOR EACH OF AN ENDLESS NUMBER OF NEW RELEASES...." *Computer Aphorisms (and memories)*

ARE YOU COMPETENT TO PRACTICE THE NEW LAW OF LAWYER TECHNOLOGY COMPETENCE?



Are You Cyber Security Competent?

Do You Practice With Someone Who Has Technophobia?

Do You Know What the Terms of Service of Your Cloud-Storage Provider Allows the Provider to Do with Your Files?

Do You Keep Up with Technology Changes Affecting the Practice of Law?

Do You Have Cyber Liability Insurance?

Professor Andrew Perlman in his article "The Twenty First Century Lawyer's Evolving Ethical Duty of Competence" (*The Professional Lawyer*, Vol. 22, No. 4) observed:

> "Technological competence is not just a disciplinary or malpractice concern. It is becoming essential in a marketplace where clients handle more of their own legal work and use non-traditional legal service providers (i.e., providers other than law firms). To compete, lawyers need to learn how to leverage "New Law" – technology and other innovations that facilitate the delivery of legal services in entirely new ways."

Professor Perlman provides these examples of New Law Technology:

- Automated document assembly,
- Expert systems (e.g., automated processes that generate legal conclusions after users answer a series of branching questions),
- Knowledge management (e.g., tools that enable lawyers to find information efficiently within a lawyer's own firm, such as by locating a pre-existing document addressing a legal issue or identifying a lawyer who is already expert in the subject),
- Legal analytics (e.g., using "big data" to help forecast the outcome of cases and determine their settlement value),
- Virtual legal services, and
- Cloud-based law practice management.

A recent Wisconsin Bar Association ethics opinion (*EF 15-01*, 3/23/2015) concerning the ethical use of cloud computing opined that:

> "(C)loud computing is permissible as long as the lawyer adequately addresses the potential risks associated with it … (L)awyers must make reasonable efforts to protect client information and confidentiality as well as to

CONTINUED ON PAGE 8

"THE BEST BOOK ON PROGRAMMING FOR THE LAYMAN IS "ALICE IN WONDERLAND"; BUT THAT'S BECAUSE IT'S THE BEST BOOK ON ANYTHING FOR THE LAYMAN." *Yale University: Epigrams in Programming*

LAWYER TECHNOLOGY COMPETENCE

CONTINUED FROM PAGE 7

protect the lawyer's ability to reliably access and provide information relevant to a client's matter when needed. To be reasonable, those efforts must be commensurate with the risks presented. Lawyers must exercise their professional judgment when adopting specific cloud-based services, just as they do when choosing and supervising other types of service providers."

The opinion includes the following considerations in determining what are reasonable efforts:

- Information's sensitivity;
- Client's instructions and circumstances;
- Possible effect that inadvertent disclosure or unauthorized interception could pose to a client or third party;
- Attorney's ability to assess the technology's level of security;
- Likelihood of disclosure if additional safeguards are not employed;
- Cost of employing additional safeguards;
- Difficulty of implementing the additional safeguards;
- Extent to which the additional safeguards adversely affect the lawyer's ability to represent clients;
- Need for increased accessibility and the urgency of the situation;
- Experience and reputation of the service provider;
- Terms of the agreement with the service provider; and
- Legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality.

The Wisconsin opinion notes that it is not possible to give specific requirements for reasonable efforts because of constant technology change. "Lawyers must exercise their professional judgment in adopting cloud based services, just as they do when choosing and supervising other types of service providers." The opinion, however, includes the following general guidance:

- Lawyers should have "at least a base level comprehension of the technology and the implications of its use." While attorneys are not required to understand precisely how the technology works, competence requires at least a cursory understanding of the technology used. Such a cursory understanding is necessary to explain to the client the advantages and risks of using the technology in the representation.
- Lawyers should understand the importance of computer security, such as the use of firewalls, virus and spyware programs, operating system updates, strong passwords and multifactor authentication, and encryption for information stored both in the cloud and on the ground. Lawyers should also understand the security dangers of using public Wi-Fi and file sharing sites.
- Lawyers who outsource cloud-computing services should understand the importance of selecting a provider that uses appropriate security protocols. "While complete security is never achievable, a prudent attorney will employ reasonable precautions and thoroughly research a cloud storage vendor's security measures and track records prior to utilizing the service. Knowing the qualifications, reputation, and longevity of the cloud-service provider is necessary, just like knowing the qualifications, reputation, and longevity of any other service provider."
- Lawyers should read and understand the cloud-based service provider's terms of use or service agreement.
- Lawyers should also understand the importance of regularly backing up data and storing data in more than one place.
- Lawyers who do not have the necessary understanding should consult with someone who has the necessary skill and expertise, such as technology consultant, to help determine what efforts are reasonable.
- Lawyers should also consider including a provision in their engagement agreements or letters that, at least, informs and explains the use of cloud-based services to process, transmit, store and access information. Including such provisions not only gives the client an opportunity to object, but also provides an opportunity for the lawyer and client to discuss the advantages and the risks. (*footnotes omitted*)

"WHY DID THE ROMAN EMPIRE COLLAPSE? WHAT IS LATIN FOR OFFICE AUTOMATION?" *Yale University: Epigrams in Programming*

OFFICER AND DIRECTOR LIABILITY FOR CYBER SECURITY ATTACKS

RUTH H. BAXTER
Crawford & Baxter, P.S.C.
President, Lawyers Mutual Insurance Company of Kentucky

Attorneys frequently serve as officers and directors of corporations, whether for their own law firms, on a community bank Board, or for a local non-profit organization. In such a capacity, they are required to discharge their duties and responsibilities in good faith and by exercising ordinary care and diligence.[1] Kentucky law explains that a director's obligation requires an assurance that a system of internal control exists that the Board believes is adequate in concept and design to ensure that appropriate information comes to the Board's attention in a timely manner so that the Board may respond appropriately.[2]

Enter the age of digitization and all aspects of business now rely upon Internet technology. With the use of such technology also comes the risk associated with it. In the last two years corporations have taken major 'hits', both financially and professionally, for cyber attacks that have resulted in the exposure and sale of personal information, medical records, and trade secrets. Shareholder derivative lawsuits have followed against the Boards of these companies seeking damages for the financial catastrophe that follows such a breach.[3] As cyber attacks are now the norm in business and commerce, a corporate officer or director must consider cyber security as a part of the fiduciary responsibility owed to the business. As Security and Exchange Commissioner Luis A. Aguilar recently stated, "Boards that choose to ignore, or minimize, the importance of cyber security responsibility do so at their own peril."

As a corporate officer or director, attorneys are often looked upon to lead the way in bringing potential risks to a Board's attention. While directors are not responsible to manage cyber security risks, they must oversee the corporation's system of internal controls to be sure that management is doing the best job possible. Board members generally are not personally liable for a failure of such oversight "... unless there is a sustained or systematic failure of the Board to exercise oversight – such as an utter failures to attempt to assure that reasonable information and reporting system exists...." (*Caremark Int'l, Inc. vs. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996)). However, where a Board has not engaged in **any** oversight of

the corporation's cyber security risk now that this risk is well-known, the directors could be individually liable for breaching their duties as outlined by *Caremark*.

Claims made against directors in pending shareholder derivative litigation where security breaches occurred have centered on two issues: First, did the directors breach their fiduciary duties by making a decision that was ill-advised or negligent, and second, did the directors fail to act when it knew or had reason to know of a cyber security threat. Allegations against corporate officers and directors have included the following inquiries:

1. Did the Board fail to implement an effective cyber security program that addressed the potential risks to the corporation?
2. Did the Board monitor its cyber security program to make sure it was current on cyber security risks in the marketplace?
3. Did the Board assure itself that management was implementing and maintaining internal controls to protect personal and financial information of the business?

CONTINUED ON PAGE 10

"THE NUMBERS CLEARLY SHOW THE **DARWINIAN PROCESS** AT WORK IN THE INTERNET. THE WEAK FALTER, WHILE THE STRONG SURGE AHEAD." *Greg Kyle*

OFFICER AND DIRECTOR LIABILITY

CONTINUED FROM PAGE 9

4. Did the corporation have a breach response in place and was the Board in agreement that reasonable steps would be made to notify clients and customers if the company's information security system had been breached?
5. When a breach occurred, did the Board require management to comply with state and federal notification statutes, and oversee information disseminated to shareholders and third parties to confirm that it was not materially false or misleading?

Despite the well-publicized data breaches for commercial businesses such as Target,[4] and government breaches at the Office of Personnel Management,[5] among others, a recent survey found that nearly one-half of corporate directors had not within the past year discussed the company's crisis response plan in the event of a breach.[6] Similarly, 67% had not reviewed the company's cyber insurance coverage, if any, and nearly 60% had not discussed hiring an outside security consultant to review its cyber security plan.[7]

To ensure that an attorney officer or director is fulfilling the good faith obligation in an informed basis, and in a manner that is in the best interests of the corporation, discussion about cyber security issues needs to be held in the Board room on a routine basis, and documented in the corporate minutes. Management of the corporation needs to be asked:

1. What are our corporations' most valuable assets? (Information? Money? Trust from clients?)
2. How is our cyber security plan protecting these assets? Is there more that can be done?
3. Do we have employee policies on using our company's Internet, cloud system, and website? Are employees being trained on these policies? Are employees aware of cyber risks for the business, and trained to identify them on our systems?
4. What cyber security controls are in place for third party vendors? Do we monitor those controls? Do we audit the third party vendors to be sure they use those controls?
5. Do we have sufficient staff, and have we budgeted sufficient funds, to address cyber security risks for the business? Is an outside consultant needed to discuss these issues with the Board?
6. Do we have a data breach response plan in place? Who is responsible for its implementation? Have we tested the plan? What role does the Board have in that plan? How do we directors respond to clients and the public about data breaches?
7. Do we have cyber liability insurance? If we do, then what does it cover? If we don't have cyber liability insurance, why did management decide not to purchase it?

While corporate Boards are comfortable in reviewing financial issues and overseeing management, unfamiliarity with cyber security issues affecting the business requires directors to become educated about the subject. A Board member doesn't need to know how to configure a firewall, but the director does have a fiduciary responsibility to understand what cyber security risks affect the corporation, and what impact a breach would have upon the organization. Discussions need to take place in the Boardroom so that all directors and officers can attest that management has taken the necessary measures to protect the company's most critical assets, and can effectively respond to a data breach. Because, as cyber security experts routinely explain, "It's not a matter of if we have a breach, but only a matter of when it will occur."

ENDNOTES

1 *Kentucky Business Corporation Act ("KBCA") KRS 271B.8-300(1); KRS 286.3-065.*

2 *KRS 271B.8-300(2).*

3 Shareholder derivative litigation for data breaches currently are pending against directors of Target Corporation; Wyndham Worldwide Corporation; TJ Companies, Inc., and Heartland Payment Systems, Inc., to name a few.

4 The breach at Target was the result of hackers exploiting the heating and air conditioning vendor it utilized.

5 Foreign hackers obtained personnel information, including fingerprints from past and present federal government employees.

6 Internet Security Alliance, NACD, "A cyber security action plan for corporate boards," *Navigating the Digital Age: The Definitive Cyber Security Guide for Directors and Officers*, Claxton Business & Legal, Inc. (October 2015).

7 *Id.*

"NEVER LET A COMPUTER KNOW YOU ARE IN A HURRY." *Unknown*

DATA BREACHES

CONTINUED FROM PAGE 3

of the network's downtime and for property damage to the firm's physical assets. Theft of the law firm's own intellectual property, however, remains uninsurable as insurance companies have struggled to understand what is the intrinsic loss value if the system is compromised.

SUMMING UP

Despite an attorney's best efforts to minimize exposure to data breaches of client information by evaluating its policies and procedures, realistically breaches will occur and law firms can experience significant financial losses associated with the breach. In today's technological world, cyber security risks affect solo practitioners and law firms of all sizes. Attorneys are placed in an unenviable position of maintaining professional responsibility to their clients, while guarding against a variety of cyber security threats, aware that despite their efforts, no defense can provide perfect protection of their valuable client information. Only by having an effective strategy to analyze those risks, mitigate their impact on your law firm, and maximize protection against data breaches, can attorneys feel confident they are doing all that they can to reasonably protect against cyber security risks.

ENDNOTES

1 This topic will be explored in greater detail at the 2016 Kentucky Bar Association Convention on Friday, May 13, 2016, in a panel discussion on "Cyber Liability Issues for Attorneys" at 9:00 a.m.

2 Chad Pinson, managing director Stroz Friedberg, a New York-based cybersecurity firm reported in *Bloomberg Newsweek* on March 19, 2015.

3 January 25, 2015, letter from Ziprick & Cramer Law Firm, Redlands, California.

4 *KRS 365.732(1)*

5 *KRS 365.732 (5)*

6 See *15 U.S.C. Section 1681a.*

7 *SCR 3.130 (1.6)*

THE RISK MANAGER
PUBLISHED BY LAWYERS MUTUAL INSURANCE COMPANY OF KENTUCKY

DEL O'ROARK
Newsletter Editor

ETHICS STILL APPLY

CONTINUED FROM PAGE 6

remains logged in. One way to manage this risk is to always log out of cloud-based programs. Then, if your phone is compromised, the data in the cloud is still password-protected.

Attorneys should also be aware of some of the more traditional cyber defense tools to protect their smartphones, such as passwords and encryption. When a strong password is coupled with encryption, some think that the device is rendered essentially secure.[11]

CONCLUSION

Technology is constantly changing, with the result that attorneys will use the Internet and cloud-computing in new and different ways in the future. For this reason, there is no one solution for complying with an attorney's ethical duties associated with cloud computing and cyber security risks. Attorneys must understand the technology they choose to use in their practice and recognize they have a professional duty of obtaining and maintaining competence in the technology that now pervades the practice of law.

ENDNOTES

1 Jake A. Thompson is a first year associate at Crawford & Baxter, P.S.C., Carrollton, Kentucky. He is a 2015 graduate of the University of Kentucky College of Law where he served as Staff Editor for the *Kentucky Journal of Equine, Agriculture and Natural Resources*, and was a member of the Moot Court Board and Trial Advocacy Board.

2 "What Kentucky Lawyers Need to Know about the Ethics and Risk Management of Cloud Computing," *The Risk Manager*, Summer 2012, citing the (The Free On-line Dictionary of Computing).

3 Pennsylvania Bar Association, Committee on Legal Ethics and Professional Responsibility, Formal Opinion 2011-200.

4 New York State Bar Association, Committee on Professional Ethics, *Opinion 842.*

5 See e.g., Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility, Formal *Opinion 2011-200*; The Florida Bar, Professional Ethics of the Florida Bar, *Opinion 12-3*; and New York State Bar Association, Committee on Professional Ethics, *Ethics Opinion 842.*

6 See e.g., Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility, *Formal Opinion 2011-200*; and Maine Board of Bar Overseers, *Ethics Opinion #207, The Ethics of Cloud Computing and Storage.*

7 Iowa State Bar Association, *Ethics Opinion 11-01.*

8 Alabama State Bar, *Formal Opinion 2010-02.*

9 *Id.*

10 *Id.*

11 Jeff Sallee, "Securing Client Data: A Business Reasonable Approach," *Bench & Bar Magazine*, Vol. 79, No. 3 (May2015).

"WHEN SOMEONE SAYS "I WANT A PROGRAMMING LANGUAGE IN WHICH I NEED ONLY SAY WHAT I WISH DONE," GIVE HIM A LOLLIPOP."

Yale University: Epigrams in Programming

Lawyers Mutual
www.lmick.com

A Exceptional Financial Stability Rating® Demotech, Inc.

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

28 YEARS LAWYERS MUTUAL 1987-2016

FOR MORE INFORMATION ABOUT
LAWYERS MUTUAL, CALL (502) 568-6100
OR KY WATS 1-800-800-6101 OR
VISIT OUR WEBSITE AT LMICK.COM.

DEAD HORSE RISK MANAGEMENT

DOES THIS DESCRIBE YOUR FIRM'S APPROACH TO RISK MANAGEMENT?

"The code of tribal wisdom says that when you discover you are riding a dead horse, the best strategy is to dismount. In law firms, we often try other strategies with dead horses, including the following: buying a stronger whip, changing riders, saying things like 'This is the way we have always ridden this horse'; appointing a committee to study the horse; arranging to visit other firms to see how they ride dead horses; increasing the standards to ride dead horses; declaring that the horse is better, faster, and cheaper dead; and finally harnessing several dead horses together for increased speed."

Charles F. Robinson quoted in the National Law Journal

DON'T MISS

"CYBER LIABILITY ISSUES FOR ATTORNEYS"

FRIDAY, MAY 13, 2016
9:00 A.M.
2016 KBA CONVENTION

This program, in the format of a panel discussion, will explore in detail cyber security issues and essential lawyer competency requirements.