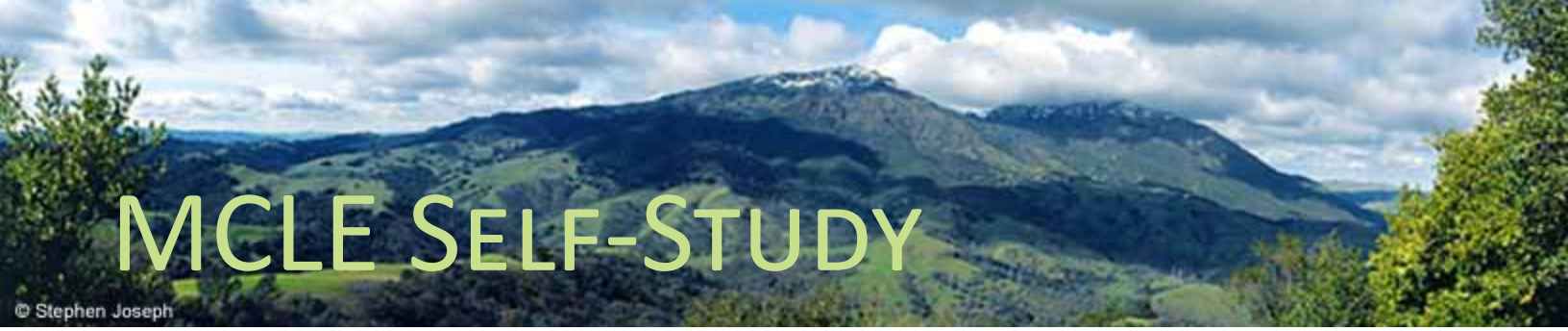

Cyber Attacks and Ethical Obligations to Clients

by Carol M. Langford

Technology as changed the way lawyers practice law. Smart phones and cloud computing mean that lawyers can draft pleadings even while on vacation in another country. Nevertheless, freedom comes with a price; here it is the threat to client data and confidential information by the fact that data and information are let out of the four corners of the bricks-and-mortar law office and put into cyberspace. The State Bar of California anticipated this problem years ago, and developed a series of Ethics Opinions to address the issues that arise with the use of technology by attorneys. They also list a series of articles, Opinions and Rules that addresses cyber security on the Bar's web site.

Ethics Opinion 2010-179 discusses whether an attorney violates the duties of confidentiality and competence she owes to a client by using technology to transmit or store confidential information when the technology may be susceptible to unauthorized access by third parties. The Opinion concludes that whether there has been a violation of ethical duties will depend on the particular technology being used and the circumstances surrounding such use. It admonishes the lawyer to evaluate: 1) the level of security attendant to the use of that technology, including whether reasonable precautions may be taken when using the technology to increase the level of security; 2) the legal ramifications to a third party who intercepts, accesses or exceeds authorized use of electronic information; 3) the degree of sensitivity of the information, 4) the possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product; 5) the urgency of the situation; and 6) the client's instructions and circumstances, such as access by others to the client's devices and communications.

The Opinion makes clear that the B&P Code section 6068 (e) duty to "maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client" is not rendered moot by the use of technology. Similarly, the duty of competence in Rule 3-110(A) applies to the attorney's diligence and learning of all things related to preserving the confidence of client matters, and it also applies to the duty to supervise the work of non-attorney employees and agents - here your IT department.

Model Rule 1.6 of the ABA Model Rules of Professional Conduct contains comments which directly address competence. Although California lawyers are not governed by the ABA Rules, courts sometimes cite to these Rules when California does not have a Rule on point. Comment 16 of Model Rule 1.6 says that a lawyer must safeguard information of a client and Comment 17 addresses the client who asks for special security measures to protect their matter and the lawyer's need to address that issue.

Sole practitioners might wonder whether large law firms are immune from attack. No, if Wiley Rein LLP in Washington D.C. is any indication of the vulnerability of all law firms. A Chinese hacker group managed to penetrate Wiley's computer system after the firm pursued unfair trade claims against exporters in China and obtained billions of dollars in tariffs on exports of solar cells. The hackers managed to get the confidential information of clients like the European Union Council, Halliburton, and a Canadian magistrate. Bloomberg News, Hackers Linked to China's Army Seen From EU to DC, Bloomberg Business, Jul. 26, 2012. Another attack occurred on a group of law firms in Toronto involved in a $40 million dollar takeover deal. The Risk of Data Breaches in Law Firms, Jett Hanna, TLIE, May, 2015. So clearly, we all are vulnerable.

The ABA has recognized that computer attacks are now picked up by IT departments of law firms on an almost daily basis because law firms are being targeted by hackers interested in learning of mergers and acquisitions, litigation strategies and patent information. As a result of that, the ABA adopted Resolution 109 which called for all law firms to implement and maintain an appropriate security program.

Data is not just accessed by overseas hackers. When a lawyer loses his phone or lap top in an airport or coffee shop it can fall into the hands of hackers too. This can be particularly devastat-

ing to the young solo practitioner who has no bricks-and-mortar office. But it happens in big law firms as well; Jett Hanna reports in the TLIE article cited above that in one Silicon Valley law firm an employee stole 200 employee lap tops, and in a Texas case computers from a law firm were found in a pawn shop.

California has enacted legislation after citizens demanded more transparency and accountability of businesses to protect their private information. Section 1798.29 of the Civil Code requires any business (that includes law firms) to disclose any breach of security where unencrypted information has been released to someone unauthorized to view it. It is very specific in how that notice must be done; for example, in at least 10-point type with clear headings. It is really nothing but a reflection of a lawyer's duty under Rule 3-500 of the Rules of Professional Conduct to keep a client informed of significant developments in a case. It would be significant that someone outside of your law firm has your client's confidential case information.

How long has it been since you pulled out your legal malpractice insurance policy and checked to see if it covers your computer getting hacked with a Ransomware virus? Those viruses can render your computer data worthless, and can put client communications into the hands of thieves. Policies differ as to whether they cover data breaches. Typically a professional liability policy insures against claims from clients for falling below the standard of care in the provision of legal services. Could that be construed to cover a data breach? Maybe, but it might not cover all the costs in repairing the damage including state penalties, forensic examinations, the costs of notifying all your clients and of providing credit monitoring.

There are now cyber liability provisions that can be bought as well as standalone policies. The coverage types and limits vary widely.

What should a lawyer do if their computer has been hacked? Simshaw and Wu, from Ethics and Cybersecurity: March 2015 on their web site, have a great list of safeguards to take including: making sure the law office has walls, doors alarms and windows that reasonably prevent physical intrusion, keeping an inventory of computing devices, wiping electronic data off such devices before they are sold or put in a dumpster, the use of strong passwords and log offs after a period of inactivity, and the use of firewalls, virus protection software and systems that log user activity. But most important, at least to the law firm, is the need for a plan for the recovery of data and notification of breach as well as a firm continuity plan to assure continued operation in the event of a cyber attack.

A lawyer can find it difficult to protect information if, for example, an employee hacker is bent on invading his system. But most hackers will be stopped at the gate and move on to easier prey if lawyers use the above fairly simple and cheap precautions.

About the Author

Carol M. Langford is lawyer who specializes in ethics and attorney conduct matters including representing clients before the State Bar. She is currently serving on the Commission to Revise the Rules of Professional Conduct and as a lecturer in law at U.C. Berkeley Boalt Hall School of Law. She is the past Chair of the California State Bar ethics committee.

MCLE Self-Study Test

To receive MCLE credit, please answer the test questions on the next page, choosing the one best answer to each question.

Mail the test page and your payment ($30* for CCCBA members / $45 for non-members) to CCCBA at the address on the test form. Certificates are dated as the day the form is received.

MCLE Self-Study

Cyber Attacks and Ethical Obligations to Clients

MCLE SELF-STUDY TEST

1. The State Bar of California has not yet addressed the issue of technology and data breeches.
   ☐ True ☐ False
2. Ethics Opinion 2010-138 addresses the duties of confidentiality and competence when using technology.
   ☐ True ☐ False
3. Lawyers should evaluate the level of security attendant to the use of technology, including whether reasonable precautions can be taken.
   ☐ True ☐ False
4. Lawyers should evaluate the legal ramifications to a third party who intercepts, accesses or exceeds authorized use of electronic information.
   ☐ True ☐ False
5. The degree of sensitivity of the information is not an important consideration in evaluating whether and what type of technology should be used.
   ☐ True ☐ False
6. Special encryption is required for clients that specifically request that certain documents remain confidential.
   ☐ True ☐ False
7. Business and Professions Code section 6068(e) addresses what is confidential information.
   ☐ True ☐ False
8. Rule of Professional Competence 3-310 addresses the duty of competence.
   ☐ True ☐ False
9. ABA Model Rule of Professional Conduct 1.6 contains comments that address competence and technology.
   ☐ True ☐ False
10. Sole practitioners follow different duties of confidentiality and competence than firms with more than three attorneys on staff.
    ☐ True ☐ False
11. A security breach must be disclosed to a client according to Rule 3-500 of the Rules of Professional Conduct.
    ☐ True ☐ False
12. Most law firms are immune from cyber attack.
    ☐ True ☐ False
13. Computer attacks are picked up by IT departments on a daily basis.
    ☐ True ☐ False
14. The California Civil Code addresses the responsibility of all businesses to protect clients' private information.
    ☐ True ☐ False
15. Insurance coverage for computer security is required for all law firms in California.
    ☐ True ☐ False

HOW TO RECEIVE ONE HOUR OF MCLE CREDIT

Answer the test questions, choosing the one best answer to each question. Mail this Self-Study and your payment ($30 per credit hour for CCCBA members/$45 per credit hour for non-members) to CCCBA at the address below. Certificates are dated as the day this form is received.

Name _____ State Bar # _____

Firm Name _____

Address _____

City, State, Zip _____

Phone _____ Email _____

☐ Visa ☐ MasterCard ☐ Amex ☐ Check (payable to CCCBA)

Cardholder Name _____

Card Number _____

Expiration Date _____

Signature _____

Contra Costa County Bar Association
2300 Clayton Road, Suite 520, Concord, CA 94520

July 2016 CCL - 1 Hour Legal Ethics MCLE Credit