A LAWYER'S ETHICAL DUTY TO IMPROVE TECHNICAL SKILLS: "IMPROVE YOUR CYBER-SECURITY WITHOUT A PhD"

CLAUDE E. DUCLOUX, *Austin*
Law Offices of Claude Ducloux

State Bar of Texas
28TH ANNUAL
ENTERTAINMENT LAW INSTITUTE
November 8-9, 2018
Austin

CHAPTER 1

This article was originally published in the Texas Bar Journal, Vol. 81, No. 9 in October 2018.

CLAUDE E. DUCLOUX
3700 Capital of Texas Highway North, Suite 300
Austin, Texas 78746
Telephone: (512) 716-8580
Telecopier: (512) 233-2388
E-Mail: cducloux@affinipay.com

EDUCATION

University of Texas, Austin, B.A., 1972
St. Mary's University, San Antonio, J.D., December 1976

BAR ADMISSIONS

Texas1977; California 1978, Colorado 2003
Various US District Courts and Circuit Courts of Appeal

EMPLOYMENT

Assistant General Counsel, State Bar of Texas: 1978-1980
Robinson, Felts, Starnes, Angenend & Mashburn; Civil Trial Attorney, 1980-1987
Wood, Lucksinger & Epstein; Civil Trial Attorney, 1987-1989
1989-2016 Hill, Ducloux, Carnes & de la Garza
2016 – pres. Attorney at Law, private practice, and Director of Education, Ethics and Compliance, Affinipay-LawPay

PROFESSIONAL ACTIVITIES

President, Travis County Bar Association (now, Austin Bar Association); 1997-1998; every officer position 92-97;
Chair, Texas Board of Legal Specialization, 1997-1998
Board Certified: Civil Trial Law, 1984; Civil Appellate Law, l987
Chair, Texas Bar Foundation 2005-2006; Secretary-Treasurer (04-05); Trustee 2004-2008
Chair, Texas Center for Legal Ethics and Professionalism: 2004-06, Trustee 2003-07
Chair, College of the State Bar of Texas; 1992-94; Vice-Chair 1990-92; Director, 1988-98,
Chair, State Bar of Texas Annual Meeting (Texas Bar Convention), 2001
Chair, United States Fifth Circuit Judicial Conference, Austin 2004
President, St. Mary's Law School Alumni Association, 2006-07, Trustee, 2001-2008.

Associate, American Board of Trial Advocates, 1999- pres.
Director, State Bar of Texas; District 9, 1998-2001; Executive Committee 1999-2001
(Outstanding 3rd Year Director Award - 2001)
Director, Austin Lawyers Care (now: Volunteer Legal Services of Central Texas), 86-89
Director, Austin Young Lawyers Association, 1984-1986
Editor, Travis County Practice Handbook, 1984, 1986
Trustee; St Mary's University, San Antonio, Texas 2007-08
Member and Founder *Bar & Grill Singers*, Lawyer Group performing musical parody across the country, and raising (through Jan 2008) $300,000 for *pro bono* causes.
Member, Supreme Court Advisory Committee on Court-Annexed Mediation, 1996-1998
Distinguished Mediator, Texas Mediator Credentialing Association, 2010
Appointed by Texas Supreme Court to Committee on Disciplinary Rules and Referenda (3 year term-Dec 2017-20)

PROFESSIONAL HONORS

Lola Wright Foundation Award for Promotion of Legal Ethics, 2013 (Statewide Award)
Gene Cavin Award for Excellence in CLE, State Bar of Texas, 2011 (Statewide Award)
Annual Professionalism Award, College of the State Bar of Texas, 2002 (Statewide Award)
W. Frank Newton Award (Statewide Annual Pro Bono Award given by State Bar of Texas), 2000
Outstanding Young Lawyer Award, 1987 (Awarded by Austin Young Lawyers Association)
Presidential Citation; State Bar of Texas, 2001 and 2006
Pro Bono Award, Volunteer Legal Services of Central Texas, 1991, 1993, 1997, 1999
Professionalism Award, Austin Bar Association, 2007
Outstanding Mentor of the Year Award, Austin Young Lawyers Association, 2007
SBOT- "Stars of the Bar" Award for Best Article Series *"Entre Nous"*, 2003

LEGAL PUBLICATIONS

"Entre Nous" commentary bar journal columns, since 1992- 108 columns published
CLE Publications,- more than 100 educational articles presented.
CLE Speeches and Presentations – Approximately 233 speeches from 01-01-2010 to 12-31-2017

MILITARY SERVICE Unites States Army; 1st Cavalry Division, 1972-1974 (Awarded Army Commendation Medal for Meritorious Service, 1974)

TABLE OF CONTENTS

A LAWYER'S ETHICAL DUTY TO IMPROVE TECHNICAL SKILLS: "IMPROVE YOUR CYBER-SECURITY WITHOUT A PhD"

Nothing strikes terror into the heart of a busy practitioner than the haunting fear of losing client information due to inadequate digital security. Hacking, viruses and the increasing danger of "Ransomware" present challenges never before experienced by our legal predecessors, who could keep client information safely under lock and key.

The facts and figures about cyber-losses across the country are startling: $325 Million to Ransomware alone estimated in 2015, with a predicted increase to $11.5 Billion in 2019. Cyber-Security Market Report, an on-line publication, estimates that cyber-crime damages will exceed $6 Trillion annually by 2021. We have already seen a string of law firms breached in 2015-2016 to obtain secrets on upcoming mergers and acquisitions. With each breach, lawyers stand to lose sensitive information, business disruption, and the complete loss of client trust.

I. WHERE DO WE START?

What steps can we all take that make sense, and, more importantly, steps that are understandable to the average practitioner, who has good intentions but a limited budget to employ experts?

First, let's understand the problem: The "insider threat" is the most significant risk that firms take. Giving all employees passwords and access to files mean that your employees can take digital copies out of the office, intentionally and often unintentionally, on portable thumb drives with more storage than ever before. Disgruntled employees account for 20% of all lost or copied data which leave a business.

Second, our demand for 24/7 access from anywhere leads to leaks over unsecure Wi-Fi and information obtained from our lost devices.

Third, our reluctance to change our passwords, and to strengthen those we have, means most of us use the same combinations for all our sites, making it infinitely easier to hack our systems.

Let's see how we can address these issues in some simple steps.

II. THE CYBER-ASSET INVENTORY:

Every lawyer should make a template of each device used by the lawyers and their support staff. (Free Templates are available for this purpose from several sources on line, but you can easily create your own). On this list the firm lists each computer and laptop, the Owner, the User, along with the make and model.

If your firm uses mobile devices or tablets (eg. iPads), those assets should be included in the inventory.

Also identified are your Internet Service Provider and your Network hardware, and how it is configured. Do you have a separate guest Wi-Fi? Who has Wi-Fi access? Is each channel password protected? How often do you change those passwords?

The purpose of this inventory is to see who has access to which devices, and see if all those people actually need access. Limiting access by changing and hardening passwords (discussed below) is a direct way to avoid the disgruntled employee from copying files for others. For example, few employees should have access to accounting information or bank accounts. Limit access whenever possible to those individuals who have a proven need to know.

A second purpose of this inventory is to ensure you are backing up information from all those devices in the case of a breach or virus. Seeing the number of devices on a page gives you checklist access to ensure each device has some means of regular backup. Also, it makes you decide where and who has access to those backups. The overall goal is to strengthen every asset in your office, limit employee access when access is not necessary, and making sure backups are updating.

III. STRENGTHENING PASSWORDS

Weak passwords are the easiest way to hack into private information. This includes networks, Wi-Fi, email and all other accounts we are forced to use every day. The experts recommend using a Password manager, which can generate very strong passwords, and you only need to remember one very strong password to access that manager program. As a general rule, in making our passwords we are told to avoid-

- Dictionary words
- Foreign words
- Slang or jargon
- Names associated with you

We should use-

- 12 or more characters
- Upper and lower case
- Numbers and symbols

IV. DUAL AUTHENTICATION

In our office, we are required to have 12-digit passwords changed every 90 days. Further, we have dual authentication if we're logging in from another computer, which means, every attempt to log-in sends a multi digit code to our cellphones to ensure that we are the person logging-in. It only takes another 20 seconds, but gives us a great sense of security. Gmail and most

providers will enable dual authentication for added security.

V. FORTIFY YOUR OFFICE NETWORK

In my CLE lectures, I humorously advise, "don't let your 15 year old set up your Wi-Fi." Sure, they'll do a better job than you will, but won't employ the standards you need, nor change the manufacturer's password. Always remember that the same rules should apply to your Wi-Fi as your email: generate a very strong password;

Require network authentication, selecting WPA2-Personal for most small practices. Most importantly, make sure you have a separate guest network, separate from your office network. Most routers support one or more guest networks. Don't use a router which does not have separate guest network capability.

VI. SIMPLE UPDATES TO YOUR COMPUTERS

Your office computers can be a treasure trove for an attacker, and there are multiple routes in, from open network connectivity to targeted malware. (A recent report revealed cybercriminals hacked an unnamed casino through its internet-connected thermometer in an aquarium in the lobby of the casino!). Fortunately there are a few key tools at your disposal to counter these threats, and you should enable them. They include:

- Automatic updates
- Antivirus/Anti-Malware
- Firewall

Don't automatically think these easy solutions have already been enabled. On Windows systems you can find them usually by going to "Control Panel →System Security" and enabling them.

Most newer computers also do "whole-drive" encryption. Check and see if you have an encryption setting, or ask your manufacturer.

VII. BE WARY OF WEBSITES YOU VISIT

Always remember to check that the website your visiting starts with "HTTPS," as that final S indicates it is secure.

VIII. DEALING WITH CLIENTS

This easy step is overlooked by most lawyers in the client interview: always ask if the client has special security needs. Will you be handling intellectual property or other specific information which requires enhanced cyber security? If so, how would THE CLIENT want that handled? It is reasonable to tell the client that you will use their special encryption software, but they must either provide it, or reimburse you for installing it. This important but overlooked step was recently discussed in depth in ABA Informal Opinion 477R, which was published in June 2017.

IX. ABA INFORMAL OPINION 477R

As technology advances, lawyers must determine whether it continues to be safe to send confidential information over the internet, or whether ADDITIONAL security methods should be implemented.

The ABA then restates the factors outlined in paragraph 18 of the Comment to Model Rule 1.6:

- The **sensitivity** of the information
- The **likelihood of disclosure** if additional safeguards are not employed
- The **cost** of employing additional safeguards
- The **difficulty of implementing** the safeguards and
- The **adverse affect** of the safeguards to the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

Upon consideration of these factors, Lawyers are directed to consider using these 7 steps to help guard against disclosure:

1. **Understand the nature of the threat.** Consider the sensitivity of the client's information and risk of cyber theft. If there is a higher risk, greater protections may be warranted.
2. **Understand how client confidential information is transmitted and where it is stored.** Understand how your firm manages and accesses client data. Be aware that use of multiple devices means multiple access points.
3. **Understand and use reasonable electronic security measures.** Use reasonable protections for client data. This may include security procedures such as using secure Wi-Fi, firewalls and anti-spyware/anti-virus software and encryption.
4. **Determine how electronic communications about clients' matters should be protected.** Discuss with the client the level of security that is appropriate when communicating electronically. If the information is sensitive or warrants extra security, consider safeguards such as encryption or password protection for attachments. Take into account the client's level of sophistication.

5. **Label client confidential information.** Mark communications as privileged and confidential to put any unintended lawyer recipient on notice that the information is privileged and confidential. Once on notice, under Model Rule 4.4(b) *Respect for Rights of Third Persons,* the inadvertent recipient would be on notice to promptly notify the sender.
6. **Train lawyers and nonlawyer assistants in technology and information security.** Take steps to ensure that lawyers and support personnel in the firm are trained to use reasonably secure methods of communication with clients. Also, periodically reassess and update security procedures.
7. **Conduct due diligence on vendors providing communication technology**. Take steps to ensure that any outside vendor's conduct comports with the professional obligations of the lawyer.

A full copy of this ABA Informal Opinion is easily downloadable, and contains excellent discussions of security precautions.

X. EMPLOYEE TRAINING

A very minimum, every law firm employee should be instructed on the nature of private information, and admonished that the law requires that no such information leave the office in any form without the approval of the supervising attorney. In my own office, my longtime legal assistant knows that, no matter how well she knows the opposing counsel, she must check with me before any private sensitive information is transmitted or delivered from our client file.

XI. THE STATE BAR OF TEXAS PDP-CLE JOINT RESOLUTION

The State Bar of Texas recognizes the critical nature of cyber security and the increasing important that lawyers have a duty to achieve knowledge and technical skills in these areas. On April 18, 2018, at the joint meeting of the SBOT Committee on Legal Education and the Professional Development Committee, the members in attendance jointly and unanimously adopted a resolution acknowledging that:

> WHEREAS, the practice of law is now inextricably intertwined with technology for the delivery of services, the docketing of legal processes, communications, and the storage and transfer of client information, including sensitive private and confidential information and other protected data;
>
> and further relating that
>
> "the continued competency of Texas lawyers to deliver services, communicate, and protect such information is dependent on technology skills and competency;
>
> That the mission of CLE should include
>
> "…information on technology, technical skills, and the implementation required to operate in a manner with enhances the ethical and competent delivery of legal services, and the security of client information."
>
> The joint resolution further explains:
>
> -…a lawyers should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology,* engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."
>
> BE IT FURTHER RESOLVED: The above committees recommend that Texas Disciplinary Rule of Professional Conduct 1.01, comment 8 be revised as follows:
>
> Maintaining Competence
>
> 8. Because of the vital role of lawyers in the legal process, each lawyer should strive to become and remain proficient and competent in the practice of law, including the benefits and risks associated with relevant technology. To maintain the requisite knowledge and skill of a competent practitioner, a lawyer should engage in continuing study and education. If a system of peer review has been established, the lawyer should consider making use of it in appropriate circumstances. Isolated instances of faulty conduct or decision should be identified for purposes of additional study or instruction.
>
> RESOLVED and unanimously adopted this 18th day of April, 2018.
>
> /s/ Xavier Rodriguez, Chair, SBOT- CLE Committee /s/Gary Nickelson, SBOT PDP Committee

XII. FINAL THOUGHTS

The need to review and enhance your firm's cyber-security is real. But a respect for the cleverness of hackers and the continuing fiduciary duty you have to protect client information should result in good habits, good processes, and implementing some relatively easy improvements to your office security. Remember the old joke: "You're not paranoid if people really are out to get you." Having been a victim of a ransomware attack myself, I treat every incoming email with care, and delete all suspicious messages immediately. If you do believe it is a real email, call the sender first when in doubt.

Let's be safe out there.

-Claude Ducloux is Board-Certified in Civil Trial and Civil Appellate Law, and serves on the Supreme Court Committee on Disciplinary Rules and Referenda. He is the National Director of Education and Ethics for LawPay in Austin, Texas.