ARTICLE: KILL THE DINOSAURS, AND OTHER TIPS FOR ACHIEVING TECHNICAL COMPETENCE IN YOUR LAW PRACTICE

March 20, 2015

Reporter
21 Rich. J.L. & Tech. 7

Length: 8125 words

Author: Antigone Peyton *

* Antigone Peyton is the founder and CEO of Cloudigy Law PLLC, an Intellectual Property and technology law firm located in McLean, Virginia. Antigone is an unabashed technophile focused on IP litigation and cutting-edge legal issues involving patents, trademarks, copyrights, and trade secrets. A longstanding member of The Sedona Conference Working Group 1 (electronic document retention and production), Antigone is a frequent speaker and lecturer on law and technology issues involving IP, social media, cloud computing, big data, and eDiscovery and a technology panelist for EmeraldPlanetTV.

Highlight

Cite as: Antigone Peyton, *Kill the Dinosaurs, and Other Tips for Achieving Technical Competence in Your Law Practice*, 21 RICH. J.L. & TECH. 7 (2015), http://jolt.richmond.edu/v21i3/article7.pdf.

Text

[*1] I. INTRODUCTION

[1] It is a challenge to practice law in the digital age. This is particularly true when a practice involves significant e-Discovery, Intellectual Property, and technology law--areas in which technical issues merge with legal ones. One of the major challenges of bringing a law practice up to twenty-first-century standards relates to dinosaur thoughts, a.k.a. an "old ways are best" mentality.

[2] Recent spectacular corporate data losses and publicized hacks highlight the frequency and scale of cybersecurity issues. [1] At least one **[*2]** leaked global surveillance effort focused on

---

[1] *See, e.g.*, Reuters, *Aramco Says Cyberattack Was Aimed at Production*, N.Y. TIMES, Dec. 10, 2012, at B2, *available at* http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-tookaim-at-its-production.html, *archived at* http://perma.cc/39WX-7L76 (noting that ″Cutting Sword of Justice″ were credited for a hack wiping data from about 30,000 computers at Saudi Arabia's national oil company, and that hackers are getting more creative, sometimes using devices that seem like everyday objects that belong in the workplace--like a cell phone charger); Greg Kumparak*This Fake Phone Charger Is Actually Recording Every Key You Type*, TECHCRUNCH (Jan. 14, 2015), http://techcrunch.com/2015/01/14/this-fake-phone-charger-is-actually-recording-everykey-you-type/, *archived at* http://perma.cc/P4TC-M846 (crediting a fake phone charger that logs the information you type on a wireless keyboard to Samy Kamkar); Kim Zetter,*Logic Bomb Set Off South Korea Cyberattack*, WIRED (Mar. 21, 2013, 7:05 PM), http://www.wired.com/2013/03/logic-bomb-south-korea-attack/, archived at http://perma.cc/3RL8-CA8Q (noting that several banks and

electronic information involving U.S. law firms, [2] and hackers' focus on high-value information repositories, like law firms, has increased. [3] These realities have sensitized clients to the importance of data protection protocols and secure infrastructure. [4] In the era of Edward Snowden, [5] WikiLeaks, [6] and global **[*3]** surveillance nets, [7] firms must vigilantly guard against unauthorized third-party access to sensitive client information and privileged communications. All of this highlights the importance of technical competence in the practice of law.

II. DINOSAURS TAKE RISKS WITH TECHNOLOGY

[3] There are many dinosaur thoughts pervading lawyers' views regarding the adequacy of their technical knowledge, practices, and systems. Dinosaurs say quaint things like:

. "Fax and e-mail are secure ways to communicate with clients."

. "It's ok to use public WiFi, as long as it's the airport, hotel, or Starbucks."

. "E-Discovery is just like paper discovery, except there's no boxes or warehouses."

. "I don't see a problem with using my firm-issued smart phone to download my favorite free game app and post comments and pictures on social media."

Dinosaur thoughts can cause trouble if Information Technology (IT) personnel or other colleagues at the firm do not temper them and educate their colleagues regarding the risks.

A. The Old World Is a Dangerous Place to Live

---

broadcasting companies were attacked by a logic bomb that wiped computer hard drives and master boot records that interrupted ATM operations in South Korea); Kim Zetter,*Sony Got Hacked Hard: What We Know and Don't Know So Far*, WIRED (Dec. 3, 2014, 4:02 PM), http://www.wired.com/2014/12/sony-hack-what-we-know/, *archived at* http://perma.cc/VL6R-TJ2V (discussing that hacktivists ″Guardians of Peace″ stole up to 100 terabytes of data from Sony, including login credentials and documents with personal employee information).

[2] *See, e.g.*, James Risen & Laura Poitras, *Spying by N.S.A. Ally Entangled U.S. Law Firm*, N.Y. TIMES, Feb. 16, 2014, at A1, *available at* http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-lawfirm. html,*archived at* http://perma.cc/AD5Y-G3FT.

[3] *See, e.g.*, Jennifer Smith, *Client Secrets at Risk as Hackers Target Law Firms*, WALL ST. J. (June. 25, 2012, 2:21 PM), http://blogs.wsj.com/law/2012/06/25/dont-click-on-that-link-client-secrets-at-risk-as-hackers-target-law-firms/, *archived at* http://perma.cc/B696-8ZBB.

[4] *See* Matthew Goldstein, *Law Firms Are Pressed on Security for Data*, N.Y. TIMES, Mar. 27, 2014, at B1, *available at* http://dealbook.nytimes.com/2014/03/26/law-firms-scrutinized-as-hacking-increases/, *archived at* http://perma.cc/6Z34-3BGL.

[5] *See, e.g.*, Glenn Greenwald, Ewen MacAskill & Laura Poitras, *Edward Snowden: The Whistleblower behind the NSA Surveillance Revelations*, GUARDIAN (June 11, 2013, 9:00 AM), http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsawhistleblower-surveillance, *archived at* http://perma.cc/D9PZ-KYCH.

[6] *See, e.g.*, Scott Shane & Andrew W. Lehren, *Leaked Cables Offer Raw Look at U.S. Diplomacy*, N.Y. TIMES, Nov. 29, 2010, at A1, *available at* http://www.nytimes.com/2010/11/29/world/29cables.html, *archived at* http://perma.cc/H9AU-D3GF.

[7] *See, e.g.*, David Ljunggren & Mike De Souza, *Snowden Files Show Canada Spy Agency Runs Global Internet Watch*: CBC, REUTERS, (Jan. 28, 2015), http://www.reuters.com/article/2015/01/28/us-canada-spyingidUSKBN0L11W520150128, *archived at* http://perma.cc/HK3N-GDBF.

[4] About a decade ago, the groundbreaking *Zubulake* series of opinions were issued. [8] These cases laid the groundwork for the concept **[*4]** that technical competence is a necessary component of effective legal representation and our ethical obligation to clients. [9] Dinosaur thoughts were not welcome in Judge Scheindlin's courtroom then, nor are they today. Now more judges are talking about the importance of technical competence, particularly when dealing with e-Discovery issues and noncompliance with increasingly complex electronic filing rules and procedures. [10] As the district court vented in *Allstate Ins. Co. v. Linea Latina de Accidentes, Inc.*,

> Every federal district now has embraced electronic filing. The days of attorneys being able to ignore the computer and shift blame to support staff in the event of an error are gone. The consequences are simply too serious. To the extent there are attorneys practicing in federal court who are under the impression that someone in the Clerk's office will comb their filings for errors and call them with a heads-up, the Court delivers this message: It is the responsibility of *counsel* to ensure that personal identifiers are properly redacted. [11]

The above-mentioned district court sanctioned a lawyer who filed a **[*5]** Complaint with attachments containing personal identifiers in unredacted form. [12] He then refiled the documents when the defendants raised a concern regarding the information that had not been redacted. [13]

[5] The second filing was not much better, as it contained removable redactions that could be deleted and expose the underlying information. [14] Counsel did not understand how to properly apply redactions to a PDF image. [15]

[6] In delivering its sanction decision, the court concluded that attorneys "who are slow to change run the very real risk of sanctions," and there was no excuse for not complying with the Federal Rule's requirement of redacting personal information from public electronic filings. [16]

B. Rise of the Technology Lawyers

[7] Lawyers need some technical competence if they are practicing law today, though the skills and knowledge needed vary widely depending on their practice areas and client needs. In fact,

---

[8] *See* Victor Li, *Looking Back on Zubulake, 10 Years Later*, A.B.A. J. (Sept. 1, 2014, 10:30 A.M.), http://www.abajournal.com/magazine/article/looking_back_on_zubulake_10_years_later, *archived at* http://perma.cc/965H-GF38 (discussing the*Zubulake* opinions and their impact on the body of case law relating to e-Discovery and a lawyer's obligations including a minimal level of technical competence).

[9] *See id*.

[10] *See, e.g.*, Baella-Silva v. Hulsey, 454 F.3d 5, 11-12 (1st Cir. 2006) (affirming a $ 50,000 sanction against a party for electronically filing a confidential settlement document and failing to take the proper precautions to preserve confidentiality in an electronically filed document that could lead to sanctions or other liabilities).

[11] Allstate Ins. Co. v. Linea Latina De Accidentes, Inc., No. 09-3681, 2010 U.S. Dist. LEXIS 124773, at *8 (D. Minn. Nov. 24, 2010).

[12] *See id*. at 3, 10-11.

[13] *See id*. at 4-5.

[14] *See id*. at 6-7.

[15] *See id*. at 5-7.

[16] 2010 U.S. Dist. LEXIS 124773, at 8-9.

in August 2012 the American Bar Association (ABA) approved a resolution that changed the ABA Model Rules of Professional Conduct (Model Rules) and included technical competency requirements. [17] This change requires lawyers to **[*6]** keep pace with "relevant technology" to comply with their ethical obligation to competently represent clients. [18]

[8] Model Rule 1.1 addresses the "client-lawyer" relationship and provides that a lawyer owes clients a duty of competence. [19] This Rule explains: "[a] lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." [20] While the Rule remains the same, Comment 8 now explains that lawyers should become educated regarding the benefits and risks associated with technology relevant to their practice. [21] This amendment to Comment 8 illustrates the ABA's desire to highlight the important role that technology plays in the practice of law today. [22]

[*7] [9] This seemingly minor change to an advisory comment is significant because the Model Rules serve as a guide for the ethical rules governing lawyers in most states, including Virginia. [23] The Model Rules now formally require lawyers in those jurisdictions following them to understand technology, including technology that relates to fulfilling e-Discovery obligations and protection of client confidences. Failure to comply with these ethics rules can lead to temporary or permanent disbarment or suspension of their license to practice law. [24]

[10] Rules aside, in-house counsel should understand the level of technical proficiency required for their internal team and outside counsel to competently represent the company's interests,

---

[17] *See, e.g.*, ABA Comm. on Ethics, Res. 105C, 1-2 (2012) (report to the House of Delegates), *available at* http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105c.authcheckdam.pdf; ABA Commission on Ethics 20/20,*archived at* http://perma.cc/S2XZ-WQS6; ABA,*ABA House of Delegates Approves Commission's Resolutions* (Aug. 6, 2012), http://www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethi cs_20_20.html,*archived at* http://perma.cc/3QF7-FL4L.

[18] MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. 8 (2014).

[19] *See id*. at R. 1.1.

[20] *Id*.

[21] *See id*. at cmt. 8 ("To maintain the requisite knowledge and skill, a lawyer 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.") (emphasis added).

[22] *See, e.g.*, Matt Nelson, *New Changes to Model Rules a Wake-Up Call for Technology Challenged Lawyers*, INSIDECOUNSEL (Mar. 28, 2013), http://www.insidecounsel.com/2013/03/28/new-changes-to-model-rules-a-wake-up-callfor-tech, *archived at* http://perma.cc/9U6Q-XT33 (noting the report accompanying the resolution suggests this was always a component of the competence standard for lawyers and that "[t]he proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent.").

[23] *See, e.g., Chronological List of States Adopting Model Rules*, ABA CENTER FOR PROF. RESP., http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/chrono_list_state_adopting archived at http://perma.cc/2AJL-EG7V (last visited Feb. 12, 2015).

[24] *See* MODEL RULES OF PROF'L CONDUCT SCOPE para. 19-20 (2014).

and they should hire accordingly. Outside counsel must receive education regarding the technologies that support the practice, clients' businesses, and best practices that minimize risks and maximize benefits associated with its use. Additionally, technical competence is important to satisfy counsel's obligations to the Court, the clients, and the opposing parties in a litigation or regulatory investigation.

[11] In short, lawyers are practicing law in a brave new world, and technology plays a starring role. Whether it is a predictive coding technology, cell phone tracking technology, or a firm's or company's communication software and systems--lawyers must roll up their sleeves and learn how to use it.

III. RUNNING THE SHOP

[12] Regardless of size, law firms are becoming more reliant on technology to manage their day-to-day activities, interact with clients, and **[*8]** find critical information among massive data repositories and across the Internet. Many cases filed in federal courts are subject to electronic document filing requirements, and state courts are following this trend. [25] With this increased use of technology, a number of risks arise that can harm a firm's reputation or result in loss of clients' data and legal liability. This paper discusses some common risks that firms should be aware of as well as ways in which they can minimize them.

A. The Nature of the Risk

[13] Law firms tend to foster a target-rich environment for data theft. [26] One important risk that law firms must anticipate--and prepare a rapid response plan for--involves security breaches. There are three major categories of reported data loss breaches involving lawyers and law firms: disposal of client records, mobile device theft or loss, and misuse of firm **[*9]** systems and security protocols. [27] Other losses can occur because of lax policies, inadequate training, or the inattention of system users. [28]

B. Data Security Technologies in the Modern Firm

---

[25] *See, e.g., Electronic Filing and Case Management*, U.S. DIST. CT. CENT. DIST. CAL., http://www.cacd.uscourts.gov/e-filing, *archived at* http://perma.cc/VX2T-JQTH (last visited Feb. 12, 2015) ("[E]lectronic filing is mandatory in all civil and criminal cases in the Central District of California.");*EFiling*, SUPER. CT. CAL. COUNTY ORANGE, http://www.occourts.org/online-services/efiling/, *archived at* http://perma.cc/JY6H-2Z2D (last visited Feb. 12, 2015) ("Pursuant to section 1010.6 of the Code of Civil Procedure, rule 2.253(b)(2) of the California Rules of Court, Orange County Superior Court Local Rule 352, and Local Rule 601.01 all documents filed by attorneys in probate, limited civil, unlimited civil, and complex civil actions . . . must be filed electronically unless the Court rules otherwise.").

[26] *See, e.g.*, Lolita C. Baldor, *FBI: Hackers Targeting Law and PR Firms*, NBC NEWS (Nov. 17, 2009, 10:58 AM), http://www.nbcnews.com/id/33991440/ns/technology_and_science-security/t/fbihackers-targeting-law-pr-firms/#.VMKMdV6hy7x, *archived at* http://perma.cc/C6LS-2GJ8 (discussing the November 1, 2009 FBI issued advisory warning to law firms that hackers were specifically targeting them); Goldstein,*supra* note 4 (discussing that in 2011, the FBI began organizing meetings with top law firms in the U.S. to highlight the cybersecurity and corporate espionage risks, particularly for firms with offices in countries like Russia and China and in 2012, security company Mandiant reported that an estimated 80% of the 100 largest American law firms had some malicious computer breach in 2011).

[27] *See* Matthew H. Meade, *Lawyers and Data Security: Understanding a Lawyer's Ethical and Legal Obligations that Arise from Handling Personal Information Provided by Clients*, 28 COMPUTER & INTERNET LAW. 1, 1 (2011).

[28] *See id*. at 2-3.

[14] Law firms often hold a high concentration of clients' most sensitive information in their files. State-sponsored hackers have been blamed for several high-profile law firm data breaches motivated by an interest in merger and acquisition information, intellectual property assets, and other sensitive strategic or competitive information. [29] This information may be easily obtainable because of the simple Account-Matter structure that law firms use to keep their client files organized. However, client systems may be difficult to understand, and it is often harder for outsiders to identify the subset of information they seek. Lawyers who have pulled a complicated client database or shared team folder can likely commiserate.

1. Password Management & Security

[15] Technology systems often require strong passwords and multi-step authentication processes upon sign-in and sign out or lock access after a period of inactivity or attempted access from a suspicious IP address. [30] **[*10]** These layers of protection are built into technology for a reason, but they can be easily circumvented by poor password management and careless security policies.

[16] Passwords should be between sixteen and twenty-four or more characters, depending upon the field limits of the software. Ideal passwords include special characters, uppercase and lowercase letters, and numbers. Firm employees should be required to change their passwords regularly and should not use the same password for all systems. Particularly for financial institution access and client data systems, the password used should be complex and unique to that system. Never keep a temporary or default password provided when receiving access to software or new hardware such as computers and routers. Some defaults are as simple as username: "admin" and password: "1234."

[17] Many people feel overwhelmed by the number of passwords they must track for personal use or firm systems. Using password management software to store passwords in one place and ensure that newly generated passwords meet certain requirements is an excellent first line of defense.

[18] Web browsers' (Chrome, Safari, Firefox, or Internet Explorer) built-in password storage systems have known security issues, [31] and they **[*11]** should be avoided. Cloud-based

---

[29] *See, e.g.*, Michael A. Riley & Sophia Pearson, *China-Based Hackers Target Law Firms to Get Secret Deal Data*, BLOOMBERG (Jan. 31, 2012, 4:37 PM), http://www.bloomberg.com/news/2012-01-31/china-based-hackers-target-law-firms.html, *archived at* http://perma.cc/T6LY-2P4N (noting that China-based hackers targeted several law firms while they were involved in a $ 40 Billion company takeover deal);*see also Breaking the Law: How Legal Firms Get Hacked*, ZEROFOX (May 20, 2014) [hereinafter *Breaking the Law*], http://www.zerofox.com/whatthefoxsays/breaking-lawlegal-firms-get-hacked/#.VMKOR16hy7x, *archived at* http://perma.cc/6CH8-C3QB.

[30] *IT Examination Handbook InfoBase: Authentication*, FFIEC, http://ithandbook.ffiec.gov/it-booklets/information-security/security-controlsimplementation/ access-control-/authentication.aspx,*archived at* http://perma.cc/V89D-978R (last visited Feb. 16, 2015).

[31] *See* Melanie Pinola, *Which Password Manager Is the Most Secure*?, LIFEHACKER (Sept. 20, 2012, 10:00 AM), http://lifehacker.com/5944969/which-password-manager-is-the-most-secure, *archived at* http://perma.cc/5FC7-YWYP (noting that Malware or tools like WebBrowserPassView can reveal passwords stored in web browsers because those systems rely on the computer login as the cypher for the encrypted password data stored by the browsers, and that web-based password

systems such as 1Password, KeePass, Roboform Everywhere, and LastPass are more robust than browser management systems and are designed to securely store passwords for websites, mobile apps, notes, credit card information, and other sensitive information. Many of these management systems can be accessed across platforms, meaning they work on computers, smartphones, and tablet devices equally well. [32] Several offer the ability to generate random secure passwords, audit your existing passwords, and analyze them to identify those that may have been compromised by major security breaches like the Heartbleed Security Bug of 2014. [33] All password management systems have potential vulnerabilities, [34] but they are better than a note stuck on your computer.

2. Data & Traffic Encryption

[19] Firms should also be using encryption technology to share information between an individual computer, mobile device, or web browser and the system or database where the information resides or a communication is sent. This is true regardless of whether the information **[*12]** is transferred over the Internet, via cellular and satellite communication channels, or using landlines.

[20] You might use a Virtual Private Network (VPN) to securely connect the computer networks for two geographically distant offices or connect to your office's systems while traveling. Some firms use VPN technologies to encrypt all of their Internet traffic, whether they are in or outside the office, to add another layer of security while the information is in transit. [35] Other variants on the VPN connection take advantage of the functionality, security, and other benefits obtained from data protection and management protocols. [36] The right protocol for a firm will depend on the firm's other security measures and infrastructure and what types of communications will be covered.

[21] Like data on the move, sensitive data at rest should also be encrypted. Media coverage of data breaches involving lost laptops that resulted in the potential exposure of very sensitive

---

managers that rely on a master password to gain access to the management system are generally more secure options);*see also* Jill Scharr, *Google Chrome's Security Flaw: How to Safely Store Passwords*, TOM'S GUIDE (Aug. 8, 2013, 11:54 PM), http://www.tomsguide.com/us/chrome-security-password-saver,review-1840.html, *archived at* http://perma.cc/K24P-UB6W (discussing Google Chrome's lack of security measures for data storage, easily allowing unwanted access to the user's password in unencrypted plain text).

[32] *Best Password Manager: Dashlane Vs Lastpass Vs 1Password Vs Roboform Vs KeePass*, A SECURE LIFE (last updated Mar. 4, 2015), http://www.asecurelife.com/dashlane-vs-lastpass-vs-1password-vs-roboform-vs-keepass/, *archived* at http://perma.cc/A4PB-9ZQ3.

[33] *See The Heartbleed Bug*, HEARTBLEED.COM, http://heartbleed.com/, *archived at* http://perma.cc/8KMU-3NAA (explaining that the Heartbleed Bug allows unwelcome individuals to read the memory of systems protected by versions of the OpenSSL software with design flaws).

[34] *See, e.g.*, Greg Kumparak, *LastPass Finds Security Holes in Its Online Password Manager, Doesn't Think Anyone Exploited Them*, TECHCRUNCH (July 11, 2014), http://techcrunch.com/2014/07/11/lastpass-finds-security-holes-in-its-online-passwordmanager-doesnt-think-anyone-exploited-them/, *archived at* http://perma.cc/P446-KECS (discussing the discovery of two security flaws in LastPass online password manager products).

[35] *See, e.g., VPN Technologies: Definitions and Requirements*, VPN CONSORTIUM (July 2008), http://www.vpnc.org/vpn-technologies.html, *archived at* http://perma.cc/724GUD48.

[36] *See id*.

client or employee information remind us that the loss of one device connected to the firm network can be catastrophic. Firm laptops and mobile devices should be protected with whole disk encryption or biometric access options and automated device wipe functions if someone tries to access the device without authorization.

[22] Certain document and data management systems and encryption technologies like File Vault, LUKS, or BitLocker give firms the option to encrypt sensitive information (like client data) where it is stored on a Mac, Linux, or Microsoft system, respectively. [37] This means that even if **[*13]** someone else--such as a disgruntled former employee or a hacker--accessed the encrypted data, they would be unable to read it without the decryption key.

[23] While it may seem obvious, the encryption key should not reside on the same system or in a location where it may be accessible to a third party, such as an employee of the cloud-computing provider hosting the document management system. Public cloud document providers such as Google Drive, Box.net, and Dropbox, which are popular client file storage solutions used by some small and mid-sized law firms, have been criticized for violating this simple data-protection rule. [38]

3. Security Vulnerabilities

[24] At a recent Black Hat security conference in Nevada, several researchers disclosed that USB drives can be corrupted with undetectable malware that infects the device and any computer it is connected to. [39] The researchers disclosed this vulnerability to the USB manufacturers months **[*14]** before the code for those attacks was published in an attempt to spur changes in the manufacturing process and fix these vulnerabilities. [40]

[25] If a firm does allow USB drives, the firm IT staff might monitor and log activity involving the USB ports of firm equipment. USB ports are a common vulnerability point for employees or

---

[37] *See* William Ruddy, *Moving on After TrueCrypt's Untimely Departure*, PHOENIX TS BLOG (June 26, 2014), http://www.phoenixts.com/blog/moving-on-after-truecrypt, archived at http://perma.cc/FQC2-8DE4. In May of 2014, TrueCrypt developers stopped supporting this open encryption software system after Microsoft terminated its support of WindowsXP. TRUECRYPT, http://truecrypt.sourceforge.net/, *archived at* http://perma.cc/R7HA-JKGJ (last visited Feb. 12, 2015) ("WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues"). Later versions of the Windows operating systems integrated support for full disk encryption and virtual disk images. Some have theorized the developers made this announcement because the encryption keys had been compromised or a "back door" had been created in response to a confidential demand from a law-enforcement or national security entity. See Dan Goodin,*Bombshell TrueCrypt Advisory: Backdoor? Hack? Hoax? None of the Above?*, ARS TECHNICA (May 29, 2014, 2:45 PM), http://arstechnica.com/security/2014/05/bombshell-truecrypt-advisory-backdoor-hackhoax-none-of-the-above/, *archived at* http://perma.cc/JCE2-4AQJ.

[38] *See, e.g.*, Hector Salcedo, *Google Drive, Dropbox, Box and iCloud reach the Top 5 Cloud Storage Security Breaches List*, CREDEON BLOG (Nov. 20, 2014, 7:00 AM), http://psg.hitachi-solutions.com/credeon/blog/google-drive-dropbox-box-and-icloudreach-the-top-5-cloud-storage-security-breaches-list, *archived at* http://perma.cc/36CD-3FJV.

[39] *See* Andy Greenberg, *The Unpatchable Malware that Infects USBs Is Now on the Loose*, WIRED (Oct. 2, 2014, 6:30 AM), http://www.wired.com/2014/10/code-publishedfor-unfixable-usb-attack, *archived at* http://perma.cc/V345-33WD.

[40] *See id*. The author's firm now has a "no thumb drive" policy because the USB attack code is public and the stakes are too high if a firm device becomes infected--the malware cannot be removed even if the USB drive is wiped and reformatted. *See id*.

unauthorized third parties to access firm systems and inject viruses or download information that should not leave the firm systems on a separate hard drive. [41] Without logging, it is hard to prove what and how much information was copied--or who did it. [42]

[26] Successful firms use a combination of human and software technical support to protect firm systems, equipment, and network against spam, viruses, and malware. If a firm allows client access to its wireless network, it may want to rethink that strategy. Once one piece of equipment is infected, it can infect every piece of equipment on the network. [43] In contrast, if every lawyer's device is "authorized" to access the firm network and the clients are relegated to a separate secured client wireless network, this provides an added layer of protection for the firm's systems and equipment. [44] As previously mentioned, it is a good idea to **[*15]** use encryption for all communications shuttled through the firm's network. A competent IT provider should be advising the firm to use security protocols that are adequate in light of the importance and sensitivity of the information that is shared on that network. [45]

4. Log History & Restricted Access

[27] Vulnerability issues arise with unsecured File Transfer Protocol (FTP) sites that use the "honor access system," systems on which any user can issue new user credentials. [46] The honor system sounds nice, but if a former employee creates new credentials for themselves and accesses information they placed on the site after leaving the company, it is hard to un-ring that bell or determine what information they took. Often FTP server log files are only kept for a specific (short) period of time. [47] If the theft is discovered after the log file is destroyed, the primary evidence of theft may be gone forever.

[28] This illustrates just one area where there is a genuine need for certain technology within the firm to be inaccessible to certain employees **[*16]** who neither need nor merit access to the

---

[41] *See* Caroline Baldwin, *USB-Connected Devices Present Cyber Vulnerabilities*, COMPUTER WKLY. (Aug. 11, 2014, 11:45 AM), http://www.computerweekly.com/news/2240226605/USB-connected-devices-presentcyber-vulnerabilities, *archived at* http://perma.cc/8JW6-P2T9.

[42] *See id*.

[43] *See Malware (Viruses et al)*, INFO. TECH.-MILLER SCH. MED. U. MIAMI, http://it.med.miami.edu/x699.xml, *archived at* http://perma.cc/8HYT-XD6B (last visited Jan. 28, 2015).

[44] *See* Jeff Beard, *Wireless Networking Best Practices: Version 2.0*, LAW TECH GURU (Aug. 1, 2004), http://www.lawtechguru.com/archives/mobile_tech_gadgets.html, *archived at* http://perma.cc/KJ6Q-5JWD.

[45] Whether using Wired Equivalent Privacy (WEP) 128-bit or WPA encryption, your IT personnel should make sure that all communications are secure. WEP is weaker and can be cracked. *See* Vangie Beal, *The Differences Between WEP and* WPA, WEBOPEDIA (June 15, 2007), http://www.webopedia.com/DidYouKnow/Computer_Science/WEP_WPA_wireless_security.asp, *archived at* http://perma.cc/TX4L-6ZTE. The only wireless encryption standards that have not been cracked (yet) are WPA with the AES (Advanced Encryption Standard) or WPA2.*See* Jason Fitzpatrick, *HTG Explains: The Difference Between WEP, WPA, and WPA2 Wireless Encryption (and Why It Matters)*, HOW-TO GEEK (July 16, 2013), http://www.howtogeek.com/167783/htg-explains-the-difference-between-wepwpa-and-wpa2-wireless-encryption-and-why-it-matters/, *archived at* http://perma.cc/Y3PP-RX88.

[46] RICK LEHTINEN, DEBORAH RUSSELL & G.T. GANGEMI SR., COMPUTER SECURITY BASICS 119 (2d ed. 2006).

[47] *See* IBM Knowledge Center, *File Transfer Protocol (FTP)*, IBM (last visited Feb. 18, 2015), http://www-01.ibm.com/support/knowledgecenter/SSB23S_1.1.0.8/com.ibm.ztpfztpfdf.doc_put.08/gtpc1/hftp.html?lang=en,*archived at* http://perma.cc/EX7T-SWN9.

information contained within it. This also demonstrates the importance of an IT manager's oversight of access history and file changes. In a utopian world, lawyers would all trust their peers to make good decisions 100% of the time, but in the real world they have a duty to verify reasonably diligent behavior when it comes to client confidences.

5. Due Diligence & Electronic Housekeeping

[29] With any data system accessible over the Internet, good physical and electronic security measures are crucial. Firms must do their research before implementing any firm data storage system on site or in the cloud. Here are some basic questions they might ask during the due diligence process:

. What is the geographic location of the data center, and what protections have been implemented at that site?

. Is someone in charge of applying patches and upgrades, particularly updates that address known security vulnerabilities and stability issues?

. What happens if the primary system goes down; is there a live, redundant backup that is geographically distant from the primary data site?

. Is there an offline backup, and how often is that backup created?

. What is the security policy and compliance protocol for the backup solution?

. Does the provider have direct access to the data, or is it pre-encrypted before being uploaded to the provider?

These are just a few of the questions a firm should cover when considering where and with whom they will store their firm and client data. Should a data breach involving firm or client information occur, the firm's diligence in choosing the data storage provider and implementing sound system policies and protections may become a central issue in triggering insurance coverage, weathering legal ramifications of the breach, and **[*17]** managing client communications after any notifications occur. [48]

[30] It is a bad idea to share passwords and login information. Often, it is considered a violation of the Terms of Service or Service Level Agreement when a lawyer or other firm employee signs or clicks through a site under another user's access credentials when purchasing a particular software product or a user license to a product. [49]

[31] In certain circumstances, such a situation can violate the Computer Fraud and Abuse Act (CFAA)--a quasi-criminal statute aimed at unauthorized access to proprietary and confidential information on computer systems--or the Stored Communications Act (SCA)--which protects

---

[48] *See* Sherilyn Pastor & Kelly Lloyd, *When Your Data Goes Viral: Insurance for Data Breaches*, CORPORATE COUNSEL (Jan. 29, 2015), http://www.corpcounsel.com/id=1202716324082/When-Your-Data-Goes-Viral-Insurance-for-Data-Breaches?slreturn=20150118121934, *archived at* http://perma.cc/HQ4M-JAXZ.

[49] *See* Doug Gross, *Facebook Speaks out against Employers Asking for Passwords*, CNN (last updated Mar. 23, 2012), http://www.cnn.com/2012/03/23/tech/socialmedia/ facebook-employers/,*archived at* http://perma.cc/9BP2-SJG7.

against unauthorized interception of electronic information if access to the stored communication was "without authorization" [50] or "exceeds authorized access." [51]

[32] Both statutes provide for civil liability in particular circumstances. [52] If an assistant or another employee who has access to **[*18]** other employees' account passwords leaves on bad terms, it will be hard to isolate and deal with their unauthorized access to the system using another person's credentials. And it is difficult to justify the decision to share passwords to the firm's IT personnel when they have to shut down a lawyer's user accounts and issue new ones, with new credentials. Just do not do it.

[33] Additionally, sometimes law firms are required (or decide) to delete client data, a litigation opponent's information, or firm electronic records. When deleting confidential records, consider servers and their backup systems, computers and mobile devices, external drives including USB drives, disks such as CD-ROMs and other non-reusable physical media.

[34] At a minimum, delete the electronic files and then empty the trash bin. Optimally, use a secure deletion method like a file shredder program that performs a permanent delete and overwrites the disk several times. [53] Physical media should be securely destroyed. [54] Firms should only keep encrypted copies of the minimum data necessary to comply with a data retention policy, legal, or business requirement.

[35] Many firms are notorious data hoarders and seem to hold old records without any legitimate business justification--such firms have a **[*19]** "sub-standard" information governance and recordkeeping model. [55] Legitimate business justifications for retaining electronic information do not include "I may need that information someday--you never know."

6. Cloud Computing

---

[50] 18 U.S.C. § 2701(a)(1) (2012).

[51] 18 U.S.C. § 1030(a)(1)-(2) (2012); *see also* Eric Matusewitch, *Your Facebook Password or Your Job?*, NNRC (July 18, 2014), http://blog.nnrc.com/your-facebook-password-or-your-job/, *archived at* http://perma.cc/8DP3-DEWN.

[52] *See* 18 U.S.C. § 2707(a)-(b) (2012) ("any provider of electronic communication service, subscriber, or other person aggrieved" by a knowing or intentional violation may recover damages or an injunction in a civil action as well as reasonable attorneys fees); 18 U.S.C. § 1030(g) (2012) ("Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.").

[53] *See* RICHARD KISSEL ET AL., NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, NIST SPECIAL PUBLICATION 800-88: GUIDELINES FOR MEDIA SANITIZATION 27-28 (rev. 1 Dec. 2014), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf, *archived at* http://perma.cc/9MP7-UQVN (relating to secure reuse of hardware after data deletion and disposal of electronic information). The National Institute of Standards and Technology (NIST) is responsible for developing information security standards and guidelines, including minimum standards for Federal information systems.*Id*. at ii.

[54] *See id*. at 36-37.

[55] *See* ARMA INT'L, GENERALLY ACCEPTED RECORDKEEPING PRINCIPLES: INFORMATION GOVERNANCE MATURITY MODEL (2013), *available at* http://www.arma.org/docs/bookstore/theprinciplesmaturitymodel.pdf, *archived at* http://perma.cc/8Q9F-PFEF; *see also* COHASSET ASSOCS., ARMA INT'L, 2013-2014 INFORMATION GOVERNANCE BENCHMARKING SURVEY FOR LEGAL SERVICES 6-7, *available at* http://www.arma.org/r1/news/2014/06/16/2013-2014-informationgovernance-benchmarking-survey-for-legal-service, *archived at* http://perma.cc/J4MG-WLS5.

[36] Many papers, blog posts, and books have been written about the benefits and risks of using cloud-computing technologies. [56] This paper will not focus on the benefits and risk analysis that should occur when contemplating adding cloud technologies to the firm's system.

[37] However, if a firm is considering a cloud computing solution, which means it will be using computing resources that are delivered over the Internet via a web browser or other interface, it needs to carefully read the documents that cover the contracts that provide the terms of the engagement with the cloud provider. [57] Some standard contracts state that the cloud provider owns the data, lack an assurance that the system will be live, or lack tools to export data once it is in the cloud system. [58]

[*20] [38] Analyze whether it is reasonable to place certain data in a cloud provider's hands if they refuse to meet the firm's needs and expectations. Also, check the firm's state bar website for current ethics opinions on this subject before moving to the cloud. At least nineteen states have issued ethics opinions that directly or indirectly address this subject. [59] All of those states have indicated that cloud computing or other similar technologies can be used in the practice of law but that reasonable care should be exercised to determine whether a particular provider is appropriate in a particular situation. [60]

[39] In considering options among cloud computing providers, a firm's investigation should delve into the question of whether the files are hidden from the cloud provider's employees. It would be a huge security risk if any employee who had access to the firm's accounts could view clients' files.

[40] A more subtle risk involves firm employees use of their personal cloud accounts to shuttle files between the office and home. Ultimately, this opportunity can be used for nefarious purposes, as was the case when one employee of a popular social gaming company allegedly stole confidential trade secrets using his personal Dropbox account before resigning from the company. [61]

---

[56] *See, e.g.*, Abby Shagin, *The Risks and Benefits of Cloud Computing*, SAP BUS. INNOVATION (Oct. 25, 2012), http://blogs.sap.com/innovation/cloud-computing/risks-and-benefits-of-cloud-computing-020025, *archived at* http://perma.cc/4GHW-NEAX.

[57] *See, e.g.*, Eric Griffith, *What is Cloud Computing?*, PC MAG (Mar. 13, 2013), http://www.pcmag.com/article2/0,2817,2372163,00.asp, archived at http://perma.cc/7R6H-8J9A.

[58] *See* Joe McKendrick, *9 Questions to Ask Before Signing a Cloud Computing Contract*, FORBES (Jan. 14, 2013, 4:00 AM), http://www.forbes.com/sites/joemckendrick/2013/01/14/9-questions-to-ask-beforesigning-a-cloud-computing-contract/, *archived at* http://perma.cc/6BYB-3Q83.

[59] *See Cloud Ethics Opinions Around the* U.S., A.B.A., http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html,*archived at* http://perma.cc/JN7T-L3YJ (last visited Jan. 27, 2015) (collection of ethics opinions around the United States that deal with questions regarding law firms' use of cloud computing).

[60] *See id*.

[61] *See* Complaint at 1-2, Zynga Inc. v. Alan Patmore, No. CGC-12-525099 (Cal. Super. Ct. Oct. 12, 2012) (a former employee transferred 760 confidential Zynga files to his personal account then uninstalled Dropbox to cover his tracks), *available at* http://tsi.brooklaw.edu/sites/tsi.brooklaw.edu/files/filings/zynga-inc-v-alan-patmore-etal/20121012complaint-zynga.pdf, *archived at* http://perma.cc/MFQ3-SRXD.

[*21] 7. Mobile Devices

[41] Many lawyers have a mobile phone attached to their hand and a tablet in their bag whenever they travel. Firm employees should use a PIN or password on their mobile device and IT managers should enable remote wiping and tracking technologies in case a device is lost or stolen.

[42] Additionally, most smartphones and tablets write a surprising amount of data to the device hard drive. [62] For instance, if a lawyer opens a client document attached to an e-mail on their phone, the device usually stores that information on the hard drive. Unlike traditional desktop systems, it is very hard to delete these types of files from the mobile device hard drive. [63] Sometimes, the entire device has to be wiped in order to delete sensitive files that can be casually accessed on them. [64]

[43] Now, I like mobile app games as much as the next person, but beware of apps that collect and share other data available on the device. Many mobile apps and mobile system software track a user's location, web browsing history, purchases, and a host of other information that you may not want to share. [65] After a number of high profile blow-ups, some privacy controls have been implemented on mobile platforms. [66] Users **[*22]** need to learn how to access these privacy controls through their system settings and review the terms for any app they download on a device.

[44] Some free apps give users access to games or information, then collect lots of data from their device. [67] Other apps deliver targeted ads based upon information that connects a person and past activities on that device. [68] These seemingly harmless mobile apps represent security

---

[62] *See* Daniel P. Dern, How to *Keep Your Smartphone (and It's Data) Secure*, COMPUTERWORLD (Apr. 22, 2014, 7:30 AM), http://www.computerworld.com/article/2488450/mobile-security/how-to-keep-yoursmartphone--and-its-data--secure.html, *archived at* http://perma.cc/AP2Q-932Q.

[63] *See id*.

[64] *See id*.

[65] *See, e.g.*, Rolfe Winkler & Elizabeth Dwoskin, *Google's New User Tracking Bridges Mobile Apps and Mobile Web*, WALL ST. J. (Aug. 7, 2014, 7:57 PM), http://blogs.wsj.com/digits/2014/08/07/googles-new-user-tracking-bridges-mobile-appsand-mobile-web/, *archived at* http://perma.cc/2G2U-3EGH.

[66] *See* Zack Whittaker, $*even Privacy Settings You Should Change Immediately in iOS 8*, ZDNET (Sept. 17, 2014, 2:30 PM), http://www.zdnet.com/article/seven-privacy-settings-you-should-change-immediately-in-ios-8/, *archived at* http://perma.cc/F4V5-9M8B; *see also* Klint Finley, *Out in the Open: How to Protect Your Secrets from Nosey Android Apps*, WIRED (Mar. 31, 2014, 6:31 PM), http://www.wired.com/2014/03/x-privacy/, *archived at* http://perma.cc/RPZ2-TN3R.

[67] *See, e.g.*, James Geddes, *Flashlight Apps are Spying on Users Android, iOs, Windows Phone Smartphones, is Yours on the List?*, TECH TIMES (Oct. 26, 2014, 7:36 AM), http://www.techtimes.com/articles/18762/20141026/flashlight-apps-are-spying-on-usersandroid-ios-windows-phone-smartphones-is-yours-on- *archived at* http://perma.cc/4SEQ-EKA3.

[68] *See* Kia Kokalitcheva, *Twitter Will Soon Track the Apps on Your Smartphone to Deliver More Targeted Ads*, VENTUREBEAT (Nov. 26, 2014, 10:09 AM), http://venturebeat.com/2014/11/26/twitter-will-soon-track-the-apps-on-your-smartphoneto-deliver-more-targeted-ads/, *archived at* http://perma.cc/83VE-QNJW.

breach risks to the firm. For example, researchers recently revealed that most of the top flashlight apps available on the Android platform are actually spyware. [69] It can be creepy once one digs into the data being collected and the surveillance that occurs with or without their knowledge.

[45] Here is another situation that illustrates the problems associated with unmanaged data collection by mobile apps. Imagine a firm lawyer takes a picture with their phone and posts it on Facebook. This may reveal their location at the time the picture was taken or when they accessed the Facebook app to post the picture. What if opposing counsel learned that lawyer is in New York the night before a big hearing because their social media post included their current location? The fact that the lawyer will **[*23]** be arguing an important motion the next day may be something they did not want to share with opposing counsel ahead of time.

8. Social Media

[46] There are many potential pitfalls associated with the use of social media or social media management apps on firm devices. Be wary of social media applications and platforms, as they are frequently invaded by cybercriminals and hacktivists. [70] Giving another application access to your credentials for one site or account could result in other linked accounts being hijacked.

[47] Facebook is a well-known example of a social media site that has seen its share of hacks and complaints about unauthorized sharing of private data with other sites and companies. [71] Even though Facebook now sends all hyperlinks through Websense first (a vast improvement), be wary of clicking on them. [72] The firm should have a social media policy and a plan for responding if client confidences or other sensitive information leave the firm through a social media outlet, and it should train everyone in the firm to be responsible ambassadors of the firm brand and client information when using social media.

[*24] 9. Travel Troubles

[48] Attorneys often travel for depositions or client meetings, and they can be most vulnerable to data breaches when on the road. Aside from remembering to encrypt traffic across open Internet connections, exercising good sense in not accessing client information in a manner that can be readily viewed or recorded by others would be wise. With the advent of smartphone

---

[69] *See* Waqas, *Flashlight Apps Stealing Personal Information Stored on Your Smartphone*, HACKREAD (Oct. 27, 2014), http://hackread.com/flashlight-apps-stealingyour-personal-information/, *archived at* http://perma.cc/C7G2-48GX.

[70] *See, e.g.*, Dan Lamothe, *U.S. Military Social Media Accounts Apparently Hacked by Islamic State Sympathizers*, WASH. POST, Jan. 12, 2015, *available at* http://www.washingtonpost.com/news/checkpoint/wp/2015/01/12/centcom-twitteraccount-apparently-hacked-by-islamic-statesympathizers/?P *archived at* http://perma.cc/94LC-AM6V.

[71] *See* Matthew J. Schwartz, *How to Hack Facebook in 60 Seconds*, INFORMATIONWEEK (June 28, 2013, 11:08 AM), http://www.informationweek.com/mobile/how-to-hackfacebook-in-60-seconds/d/d-id/1110576?, *archived at* http://perma.cc/G8N2-ZUPE; *see also* Fred Stutzman, Ralph Gross & Alessandro Acquiti, *Silent Listeners: The Evolution of Privacy and Disclosure on Facebook*, 4 J. PRIVACY & CONFIDENTIALITY, no. 2, 2012, at 7, 7.

[72] *See Breaking the Law, supra* note 29 (noting that social media engineering is an effective method for hacking law firms when employees click on links in social media postings with messages aimed at persuading them to access the link).

cameras and the ready availability of lapel cameras, a traveling lawyer would be wise to wait for the privacy of their hotel room to open and work on documents containing privileged information or work product.

[49] It is easy to look over someone's shoulder at the airport, on the plane, or in the hotel lobby. And it can be particularly dangerous to rely on public WiFi or hotspots when traveling--they are often unencrypted and an excellent target for eavesdroppers who want to capture data packets and login credentials for any sites others access while on that WiFi network. [73] For instance, the recent "Darkhotel" espionage campaign effectively targeted traveling business executives using hotel WiFi. [74]

[50] Another key point to remember when traveling is that many cellular providers give users the ability to turn their smartphone into a hotspot, but this does not protect their Internet traffic in any way. Using an unsecured mobile device as a WiFi hotspot for accessing the Internet on a laptop is a security concern. Anyone within range can eavesdrop on the data a traveling lawyer sends or receives from the Internet and the mobile **[*25]** device. [75] Some of the larger WiFi hotspot networks are secured (not open) and use enterprise-level security to protect a wireless connection on that network from eavesdroppers. [76] These networks are a safer option.

[51] Additionally, in the U.S., many large cellular providers encrypt the data traffic traveling to and from cell towers and the cellular device. This connection may be slower than a traditional WiFi connection, but the security benefits are significant. Finally, a VPN connection can be used on both WiFi and cell data connections. Under these circumstances, all of the user's Internet traffic and passwords travel through an encrypted tunnel, and already encrypted traffic enjoys double encryption.

10. Insurance and Audits

[52] Law firms have heightened responsibility for maintaining the confidentiality of client information because of their professional ethical requirements. What should law firms be doing to better protect their data and deal with discovered breaches after they occur?

[53] The firm should consider whether it needs cyber insurance to protect against the possible consequences of a breach. Most general liability or professional liability insurance policies (and

---

[73] *See* Michael Kassner, *Convenience or Security: You Can't Have Both When it Comes to Wi-Fi*, TECH REPUBLIC (June 24, 2013, 1:09 AM), http://www.techrepublic.com/blog/it-security/convenience-or-security-you-cant-haveboth-when-it-comes-to-wi-fi/, *archived at* http://perma.cc/4BEX-P8H6.

[74] *See* Press Release, Kaspersky Lab, Kaspersky Lab Sheds Light on "Darkhotel," Where Business Executives Fall Prey to an Elite Spying Crew (Nov. 10, 2014), available at http://usa.kaspersky.com/about-us/press-center/press-releases/kaspersky-lab-sheds-light-"darkhotel"-where-business-executives, *archived at* http://perma.cc/PH46-Y7LK.

[75] *See, e.g.*, Eric Geier, *Here's What an Eavesdropper Sees When You Use an Unsecured Wi-Fi Hotspot*, PC WORLD (June 28, 2013, 5:35 AM), http://www.pcworld.com/article/2043095/heres-what-an-eavesdropper-sees-when-youuse-an-unsecured-wi-fi-hotspot.html, *archived at* http://perma.cc/33BF-ZFUV.

[76] *See Wi-Fi Hotspots: Connecting While Traveling*, NORTON, http://us.norton.com/travel-hotspot-security/article, *archived at* http://perma.cc/A6Y5-T4AD (last visited Feb. 18, 2014).

even umbrella business insurance policies) do not cover the cost of investigating a data breach, taking remedial steps to fix the problem, or notifying those who may be affected by it. Cyber insurance policies are becoming more prevalent in many industries.

[54] Additionally, the firm might hire someone to test the systems and **[*26]** determine technical and human areas of vulnerability. Security audits may highlight practices or systems that should be changed in order to reduce these risks before a breach occurs.

11. Hardware Vulnerabilities

[55] As computer equipment ages and is replaced, it is vital to wipe all hard drives according to industry standards before either disposing of, or donating, those computers. The Department of Defense DoD 5220.22-M (ECE) recommends seven complete wipes, [77] and there are a number of free or low cost products that can be used to wipe computers and external hard drives.

[56] Every typical law office has a multi-function copier/scanner that is networked, and these devices always contain a hard drive with a copy of every page that has been either scanned or copied. These represent a huge security risk for several reasons. First, they are risky from a data perspective because of the massive number of stored documents sitting on an unencrypted hard drive in the machine. [78] Second, their networked permissions often provide access to computers, but the copier/scanner itself has low security measures required to gain access. People think nothing of leaving their copier code on a sticky note next to their computer--after all, what harm could that pose? This means anyone who can gain access to the office can access the network through this simple "backdoor" methodology.

[*27] III. WHAT IT TAKES TO PRACTICE LAW IN THE 21ST CENTURY

[57] Law firms are becoming more reliant on technology to manage their day-to-day activities, interact with clients, and work on the substantive aspects of their job. Now that we have identified dinosaur thoughts relating to technology, how do we extinguish them in the practice of law? Well, initially, lawyers must purposefully focus on education initiatives involving relevant technology. Extinguishing dinosaur thoughts also involves raising the bar and hiring good people who understand and embrace technology, then making them an integral part of the team. Ultimately, law firms must become better stewards of their clients' sensitive information and have protocols for holding or accessing it.

[58] Security breaches do not occur at one single point of failure, but at several points. Thus, a firm should verify that its IT provider is undertaking reasonable efforts to protect firm systems and equipment and ensure that firm employees are educated on those systems. Finally, firms need to understand and take advantage of the security measures that are already built into the systems.

---

[77] *See, e.g., Erase Hard Disk Wipe Parameters*, KILLDISK, http://www.killdisk.com/notes.htm, (last visited Mar. 5, 2015) (describing the U.S. Department of Defense DoD 5220.22-M (ECE), a seven pass overwriting algorithm used to erase data).

[78] *See* Armen Keteyian, *Digital Photocopiers Loaded with Secrets*, CBS NEWS (Apr. 19, 2010, 6:12 PM), http://www.cbsnews.com/news/digital-photocopiers-loaded-withsecrets/, *archived at* http://perma.cc/GVD6-7H8E.

[59] Diverse teams with different and complementary technical skills help law firms keep up with technology and continually evolve their practice. As technology continues to take a starring role in firm infrastructure, processes, and communication channels (and clients' businesses), lawyers must adapt and keep up with those changes--or go the way of the dinosaurs.