Ethics 20/20, Security, and Cloud Computing

Contents

CLOUD? SAAS? WHAT DOES IT ALL MEAN?......................................................................................................................... 2
CLIENT DATA IN THE CLOUD................................................................................................................................................... 2
IS THAT ETHICAL? ................................................................................................................................................................. 2

AMENDMENT REGARDING A LAWYER’S DUTY OF COMPETENCE (RULE 1.1).............................................................. 2
AMENDMENT TO THE RULE ON CONFIDENTIALITY OF INFORMATION (RULE 1.6) ..................................................... 3
DEFINING “REASONABLE” IN RULE 1.6............................................................................................................................ 4
RESPONSIBILITIES REGARDING NONLAWYER ASSISTANCE (MODEL RULE 5.3).......................................................... 4

THE STATES WEIGH IN ............................................................................................................................................................ 5
25 QUESTIONS FOR SAAS VENDORS................................................................................................................................... 8

CLOUD STANDARDS............................................................................................................................................................. 9
RISK MANAGEMENT IN THE CLOUD..................................................................................................................................... 9

PASSWORDS ............................................................................................................................................................................. 10
TWO FACTOR AUTHENTICATION ......................................................................................................................................... 10
ENCRYPTION........................................................................................................................................................................... 10
PRACTICE SAFE PATCHING ................................................................................................................................................. 10
REVOKING POWER............................................................................................................................................................... 11

AVOID TARGETED ATTACKS .............................................................................................................................................. 11
CURRENT (TECHNOLOGY) AWARENESS ........................................................................................................................... 12
SECURITY BREACH LEGISLATION........................................................................................................................................ 12
SECURITY POLICIES............................................................................................................................................................ 13

LOOKING FORWARD............................................................................................................................................................ 14
In recent years, Software as a Service (SaaS) and cloud technology have become increasingly popular alternatives to traditional legal software, particularly for solo and small firm practitioners. In fact a recent LexisNexis study regarding cloud computing foretells that 2014 will be “the year of the cloud”. In the ABA’s 2013 Legal Technology Survey Report (Vol. II: Law Office Technology) there was an increase of 10% in affirmative usage of SaaS from 2012 to 2013. But is it ethical to put your client data in the cloud?

**CLOUD? SAA S? WHAT DOES IT ALL MEAN?**

Loosely defined, Software as a Service (SaaS) or “cloud computing” refers to software that you access online via a web browser (like Chrome or Firefox) rather than installing directly onto your computer. The cloud is enabled by a vast network of web servers and data centers located throughout the world.

While the concept may seem alien to you, you might be surprised to learn that you likely already use some form of cloud computing in your daily work. Any web-based e-mail service (Google Mail, Yahoo) is considered cloud computing, and online legal research tools like Westlaw and LexisNexis are really the original legal SaaS -- legal research software delivered via the web.

**CLIENT DATA IN THE CLOUD**

One of the defining -- and for lawyers, the most alarming -- characteristics of SaaS is that SaaS solutions store data in the cloud rather than on the user's computer. In other words, when you use a web-mail service like Gmail, your actual emails reside on a remote served hosted by Google rather than on your own hard drive. If the emails in question are confidential client communication, or if they contain sensitive document attachments relating to an ongoing case, some concern is understandable.

**IS THAT ETHICAL?**

The ABA Ethics 20/20 Commission proposed changes to the ABA Model Rules of Professional Conduct that were adopted by the ABA House of Delegates in August 2012. These changes were recommended due to advances in technology that required tweaks to the rules to maintain relevancy. The following amended rules contain updated language that encompasses aspects of cloud computing and generally use of technology by the legal profession.

**AMENDMENT REGARDING A LAWYER’S DUTY OF COMPETENCE (RULE 1.1)**
Because technology use in law firms is now ubiquitous, the Commission proposed and the House adopted an amendment to Comment [8] of Model Rule 1.1 to remind lawyers that to be competent includes not only staying abreast of changes in the law and its practice, but also includes having a basic understanding of the benefits and risks of relevant technology. In terms of using cloud computing this update to the amendment makes clear that an attorney or law firm should be versed in the implications of technology used in the course of representation, including knowing any limitations of her personal understanding and hiring appropriate professionals to help make informed choices.

**Amendment to the Rule on Confidentiality of Information (Rule 1.6)**

The **newly adopted changes** clarify that lawyers should take reasonable precautions to protect client confidences from inadvertent or unauthorized access or disclosure (Model Rule 1.6), and identify the factors that lawyers should consider when determining whether they have taken reasonable precautions.

To help lawyers better understand how to protect client confidences in a digital age, the Commission proposed and the House adopted a new black letter paragraph (c) to Model Rule 1.6. This new paragraph clarifies that lawyers have a duty to take reasonable precautions to protect client confidences not only from inadvertent or unauthorized disclosure but from inadvertent or unauthorized access.

Because technology has so enhanced the importance of lawyers’ confidentiality responsibilities, the Commission believed it was important to elevate this information from the Comment to the black letter of the Rule.

During the Commission’s debate the Commission’s reporter Professor Andy Perlman maintained notes on the Legal Ethics Forum blog with a **summary of the rules changes** that were to go before the ABA House of Delegates. The summary provides some useful examples that are not in the amended rule, and show the thought process of the Commission:

“The proposal identifies three types of problems that can lead to the unintended disclosure of confidential information. First, information can be inadvertently disclosed, such as when an email is sent to the wrong person. Second, information can be accessed without authority, such as when a third party “hacks” into a law firm’s network or a lawyer’s email account. Third, information can be disclosed when employees or other personnel release it without authority, such as when an employee posts confidential information on the Internet. Rule 1.6(c) is intended to make clear that lawyers have an ethical obligation to make reasonable efforts to prevent these types of disclosures, such as by using reasonably available administrative, technical, and physical safeguards.
DEFINING “REASONABLE” IN RULE 1.6

The standard of care for confidentiality has long been determined by what is reasonable, however it was left to the discretion of attorneys to determine the definition of “reasonable". In the updated Comment [16] to Rule 1.6 the Commission proposed and the House approved a five point “checklist" for determining reasonableness of lawyer efforts to maintain confidentiality:

1. Sensitivity of information
2. Likelihood of disclosure without safeguards
3. Cost of additional safeguards
4. Difficulty of implementing safeguards
5. Extent to which the safeguards adversely affect lawyer’s ability to represent clients

Mere disclosure, by itself, does not trigger discipline. In discussing the duties under Rule 1.6 the Commission made it clear that they understand that lawyers can’t guarantee electronic security any more than they can guarantee the physical security of documents stored in a file cabinet or offsite storage facility. Just like fires and floods, computer systems can suffer catastrophic events or they can be hacked. The new Rule does not impose a duty on lawyers to achieve the unattainable.

Importantly, mere inadvertent or unauthorized disclosure of, or unauthorized access to this information does not, by itself, constitute a violation of the Rule. As we’ve seen recently, even the most security conscious entities can be hacked.

Further language in Comment [16] echoes the language found in some of the state level cloud computing ethic opinions, mainly:

“A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client’s information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer’s duties when sharing information with nonlawyers outside the lawyer’s own firm, see Rule 5.3, Comments [3]-[4]. “

RESPONSIBILITIES REGARDING NONLAWYER ASSISTANCE (MODEL RULE 5.3)

In addition to the updates and clarifications to the Model Rules 1.1 and 1.6 the changes to Model Rule 5.3 seems to contemplate the use of cloud computing most directly. The rule itself has been changed from “Responsibility Regarding Nonlawyer Assistants” to “Responsibility Regarding Nonlawyer Assistance” to encompass supervisory responsibilities of an attorney not
only of internal staff, but consultants, outside parties, and companies who provide services to
the law firm. To that end two entirely new comments (Comments [3] and [4]) have been added
to the rule regarding supervision of nonlawyers outside the firm. The new comments speak
directly to a law firm’s use of cloud computing:

“Comment [3]: A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering
legal services to the client. Examples include the retention of an investigative or
paraprofessional service, hiring a document management company to create and maintain a
database for complex litigation, sending client documents to a third party for printing or
scanning, and using an Internet-based service to store client information. When using such
services outside the firm, a lawyer must make reasonable efforts to ensure that the services are
provided in a manner that is compatible with the lawyer’s professional obligations. The extent
of this obligation will depend upon the circumstances, including the education, experience and
reputation of the nonlawyer; the nature of the services involved; the terms of any arrangements
concerning the protection of client information; and the legal and ethical environments of the
jurisdictions in which the services will be performed, particularly with regard to confidentiality.”

THE STATES WEIGH IN

The state ethics opinions that touch on the tenants of cloud computing generally agree that
lawyers should maintain reasonable care in evaluating the services of a cloud or third party
provider. The ABA Legal Technology Resource Center maintains a list of cloud ethics opinions
with a summary and links to the opinions at www.lawtechnology.org.

Some states have tackled cloud computing ethics opinions directly; many have provided
guidance on using cloud services indirectly. About 18 jurisdictions have ethics opinions
regarding use of the cloud. All say it is ok, as long as you investigate the products and methods
you use and keep up with changes the providers may make. In some cases they recommend
notifying your clients. For those delivering services virtually, or simply sharing files, it would
probably be a best practice to notify your clients in the engagement agreement.
Here is a sample of different cloud ethics opinions and how they are approaching the topic spanning from records management to privacy and backup:

• The New York State Bar Association Committee on Professional Ethics concluded that a lawyer may use a “cloud computer data backup system to store client files provided that the lawyer takes reasonable care to ensure that the system is secure and that client confidentiality will be maintained.” See Opinion 842 (9/10/10). In 2008 NYSBA issued Opinion 820, aka the Gmail opinion, regarding using an email service provider that scans emails for advertising purposes. In digest they concluded: “A lawyer may use an e-mail service provider that conducts computer scans of e-mails to generate computer advertising, where the e-mails are not reviewed by or provided to human beings other than the sender and recipient.”

• The State Bar of California Standing Committee on Professional Responsibility and Conduct issued Formal Opinion 2010-179 which contemplates whether an attorney violates the duties of confidentiality or competence when using technology to transmit and store client information when it may be susceptible to unauthorized access by third parties. They conclude that this will depend on the particular technology being used and the circumstances surrounding such use.

• Alabama Opinion 2010-02; “The Disciplinary Commission agrees and has determined that a lawyer may use “cloud computing” or third-party providers to store client data provided that the attorney exercises reasonable care in doing so. The duty of reasonable care requires the lawyer to become knowledgeable about how the provider will handle the storage and security of the data being stored and to reasonably ensure that the provider will abide by a confidentiality agreement in handling the data. Additionally, because technology is constantly evolving, the lawyer will have a continuing duty to stay abreast of appropriate security safeguards that should be employed by the lawyer and the third-party provider.

• Arizona Opinion 09-04 opined that”lawyers providing an online file storage and retrieval system for client access of documents must take reasonable precautions to protect the security and confidentiality of client documents and information. Lawyers should be aware of limitations in their competence regarding online security measures and take appropriate actions to ensure that a competent review of the proposed security measures is conducted. As technology advances over time, a periodic review of the reasonability of security precautions may be necessary.”

• In Massachusetts Opinion 05-04 the committee determined that “A law firm may provide a third-party software vendor with access to confidential client information stored on the firm’s computer system for the purpose of allowing the vendor to support and maintain a computer software application utilized by the law firm.”

• Nevada Opinion 33 (2006) states “the attorney’s electronic client files, which contain confidential client information and communications, are stored on a server or other computer device which is physically located and maintained by a third party outside the attorney’s direct control and supervision. It is assumed that the attorney can, as part of his or her service contract with the third party, require that all reasonably necessary means be employed by the third party to preserve the confidentiality of the information
and to prevent unauthorized access to it and disclosure of it. It is also assumed, however, that employees of the third party agency will, by virtue of their employment, have access, both authorized and unauthorized, to the confidential client information.”

- **New Jersey Opinion 701 (2006)** suggests that New Jersey lawyers may maintain client files electronically with a third party as long as the third party has an enforceable obligation to preserve the security of those files and uses technology to guard against reasonably foreseeable hacking.

- After multiple years of debate, North Carolina State Bar adopted [2011 Formal Ethics Opinion 6](#) on “subscribing to Software as A Service while fulfilling the duties of confidentiality and preservation of client property”. In summary they found that as long as steps are taken to minimize the risk of inadvertent or unauthorized disclosure of confidential client information, lawyers can use SaaS, invoking the “reasonable care” standard.

- **Pennsylvania Formal Opinion 2011-200** covers use of “the cloud” including web-based email. The committee says that attorneys can ethically store confidential client material in the cloud, provided the attorney takes reasonable care to ensure confidentiality is maintained and reasonable safeguards are employed to protect the data from breaches, loss, and other risks. In part C of the opinion a number of suggestions for what the standard of reasonable care may include, such as limiting information that is provided to others to what is required, needed or requested, ensuring that a cloud provider explicitly agrees that it has no ownership or security interest in the data, will notify the lawyer if requested to produce data to a third and provide the lawyer with the ability to respond before the information is produced, and more.

- **Oregon Formal Opinion no. 2011-188** is called “Information Relating to the Representation of a Client: Third-Party Electronic Storage of Client Materials” and says in part: Lawyer may store client materials on a third-party server so long as Lawyer complies with the duties of competence and confidentiality to reasonably keep the client’s information secure within a given situation. To do so, the lawyer must take reasonable steps to ensure that the storage company will reliably secure client data and keep information confidential. Under certain circumstances, this may be satisfied though a third-party vendor’s compliance with industry standards relating to confidentiality and security, provided that those industry standards meet the minimum requirements imposed on the Lawyer by the Oregon RPCs.

- **Vermont Opinion 2010-6**, under “Confidences of the Client” the opinion states “Vermont attorneys can utilize Software as a Service in connection with confidential client information, property, and communications, including for storage, processing, transmission, and calendaring of such materials, as long as they take reasonable precautions to protect the confidentiality of and to ensure access to these materials”.

- Maine’s Board of Overseers of the Bar writes in [Opinion #194](#) about client confidences regarding confidential firm data held electronically and handled by technicians for third party vendors. They conclude: “with appropriate safeguards, an attorney may utilize transcription and computer server backup services remote from both the lawyer’s physical office and the lawyer’s direct control or supervision without violating the attorney’s ethical obligation to maintain client confidentiality.”
Iowa Ethics opinion 11-01 regarding “Use of Software as a Service – Cloud Computing” points to Comment 17 to Iowa's Rule 32:1.6 as establishing a "reasonable and flexible approach to guide a lawyer’s use of ever-changing technology”. It recognizes that the degree of protection to be afforded client information varies with the client, matter and information involved. But it places on the lawyer the obligation to perform due diligence to assess the degree of protection that will be needed and to act accordingly.

25 QUESTIONS FOR SaaS VENDORS

It’s important to carefully examine all technology before buying, whether it’s SaaS or traditional. Here are 25 questions you should be sure to ask any SaaS vendor before committing your data to their hands. Vendors that aren’t willing or able to answer these questions should be treated with caution.

1. Are there changes in your security protocols when data is accessed, manipulated, downloaded or shared through mobile devices?
2. What training options are available for customers?
3. What kind of documentation (e.g. knowledge base, product manual) is available for your product?
4. How often are new features added to your product?
5. How does your software integrate with other products on the market, especially products in the legal market?
6. How many attorneys are currently using your product?
7. Is data from my firm to your service encrypted in transit and at rest?
8. Do you offer a Service Level Agreement (SLA) and/or would you be willing to negotiate one?
9. What types of guarantees and disclaimers of liability do you include in your Terms of Service?
10. How do you safeguard the privacy/confidentiality of stored data?
11. Who has access to my firm’s data when it’s stored on your servers?
12. Is my firm’s data hosted on servers owned and operated by your company or is it stored at another facility such as RackSpace, Amazon or Google?
13. Have you (or your data center) ever had a data breach?
14. Will we be notified if there is a data breach?
15. If you are served with a subpoena will we be notified?
16. If served with a subpoena that includes our data will we have a chance to contest the disclosure of privileged and confidential information?
17. How often, and in what manner, will my data be backed up?
18. What is your company’s history – e.g., how long have you been in business and where do you derive your funding?
19. Can I remove or copy my data from your servers in a non-proprietary format?
20. Where does my data reside – inside or outside of the United States?
21. What happens to my data if your company is sold or goes out of business?
22. What happens to my data if I stop paying monthly fees?
23. Do you require a contractual agreement for a certain length of service (e.g. 12 months, 24 months)?
24. What is the pricing history of your product? How often do you increase rates?
25. Are there any incidental costs I should be aware of?

CLOUD STANDARDS

There are very few standards that exist for cloud computing providers so that a law firm can feel comfortable in making a decision to use a service because they can display a certain certificate or accreditation indicating compliance with a prescribed set of controls and security protocols. In fact, certain catch phrases such as “SAS 70 Type 2 Certification” are misleading. If you see “SAS 70 Type 2 Certification” know that SAS 70 has been superseded and it was never a certification. It is an audit report (Statement on Auditing Standards) developed by the American Institute of Certified Public Accountants (AICPA) and was superseded by SSAE16, with the SOC2sm report generated by the auditor. Further it is highly unlikely that the vendor would share the results of the report and there is no pass/fail per se. Other standards being developed include ISO 27000 series (ISO 27001 (information security management) – 27006) and some others from the federal government, as well as regulations requiring compliance such as HIPAA and HITECH. There are also third party certifications from providers like Trust – E and Verisign, but ultimately there is not currently one single seal of approval that would put a law firm at ease for using a particular product. There are, however, a number of efforts to create complete standards. One entity that is coming close to an overall standard for cloud computing is the Cloud Security Alliance, which currently has a self-assessment, a certification and attestation, and the STAR registry of entities that have agreed to offer transparency and assurance by posting results of their self-assessment and certifications.

RISK MANAGEMENT IN THE CLOUD

Entrusting confidential client data and personally identifiable information to a third party has always held risk. Even in the days of paper and offsite storage of physical files there has been risk of exposure. The risks have shifted, have become more complex, and may have somewhat grown. However, per the updated comment [8] to the ABA’s Model Rule 1.1 Competence the duty is “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”. In addition to maintaining awareness of any relevant ethics opinions on cloud computing and a thorough investigation of any company you do business there are steps you can take to mitigate risk in the cloud, and using technology in general.
Maintaining firewalls and up-to-date anti-virus and anti-malware, maintaining vigilance when opening attachments and surfing the Internet, scrutinizing the security protocols of cloud providers, maintaining adequate backup files, and keeping operating systems patched are all vital whether or not your firm uses cloud based SaaS or on premise storage.

PASSWORDS

Your first line of defense is a good password – and lots of them. No matter how convenient using the same password for Gmail, Facebook, your online practice management, and your computer can put you at great risk. Just read Google’s Matt Honan story from Wired Magazine. Good passwords are over 12 characters long, and include symbols and numbers. Don’t use dictionary words and don’t store your passwords on your desktop! There are a variety of password managers to help you with this hurdle. Some come with the security suites. Others, such as LastPass, KeePass, Roboform and 1Password are separate and have different features and functions.

TWO FACTOR AUTHENTICATION

Another option to safeguard access to your accounts is two factor authentication. Available for Gmail, Dropbox, LastPass, WordPress and more, two factor authentication allows someone to access a program armed with something they know (a password) and something they have (usually a mobile phone). In order to access your account you would need both, reducing the chance that someone who is NOT you will access your account. See the article “Set Up Two Factor Authentication: What Are You Waiting For?” for a quick tutorial on using it with major online services.

ENCRYPTION

There are third party encryption tools that allow you to encrypt documents and emails as necessary, especially when using free, consumer based products like Dropbox or Gmail that may have terms of service and privacy policies that run counter to confidentiality concerns. For encrypting files stored in online repositories such as Dropbox, Google Drive, or SkyDrive tools like Viivo or BoxCryptor let you easily encrypt and decrypt documents you save with an online service provider. SendSecure, Enlocked, SecureGmail, Rpost and others let you encrypt email – and its attachments – easily and for free. If the data you are sending or storing is highly confidential consider these means of extra protection. See the “How To” videos on using easy email encryption tools and using BoxCryptor to encrypt files stored in Dropbox, Google Drive, etc..

PRACTICE SAFE PATCHING
Recently headlines have been buzzing with zero day exploits, including those for Java and Internet Explorer. While these exploits have made news, many others do not. It is essential to keep all applications, add-ons, and applets patched on your machine. Easy targets for hackers include Adobe Flash, Apple’s QuickTime, Adobe Reader, and the aforementioned Oracle Java. These programs run in the background most of the time in your browser and are usually called up only when needed by a web site. Do not ignore reminders to update these applications. If you are unsure whether the message to update is in itself a virus a quick Google search will usually confirm whether a patch has been issued.

REVOKEING POWER

In many large organizations end users do not have administrative privileges on their machines. IT departments can reduce security threats by locking down computers on the network so that they do not have the permission to actually install anything. Most people are resistant to this policy, so IT is constantly battered with requests to make an exception, just for them. However, this is one of the best ways to keep a computer from unintentionally installing malware or viruses in the background. While Apple’s OS X and Windows 7 have made major strides in alerting the user to provide permission to install software, these alerts will also be bypassed by smart viruses. By removing administrative rights, this threat is significantly reduced. Even solos running non-networked computers should set up the system so that the primary login does not have administrative rights.

Another tactic, which is considered “security through obscurity” rather than an actual security software or policy, is to change administrative defaults and privileged accounts. When possible change the default administrative name, ports, or directory names for things like routers, network installed software, individually installed software, or network shared ports.

All mobile devices that have the ability to connect with the firm’s network (including via Outlook Exchange or Dropbox) must have strong password protection, and the firm must be able to remotely wipe the date. Firm policy should require that users notify IT staff or the office administrator if the device is lost or stolen immediately.

AVOID TARGETED ATTACKS

Firms must maintain constant vigilance against social engineering, and train all staff and lawyers to be wary. Social engineering is a method of tricking a person to open the door for malicious attacks, and usually prey on fear, vanity, or the desire to help someone in need. You have all seen them: the direct message from Twitter from someone you know asking “what are you doing in this video?”; the email from a friend needing you to send money via electronic transfer
because she lost her wallet while traveling outside of the country; the email from the Better Business Bureau requesting you to click through to see a negative report that has been filed; and the list goes on. Learn to recognize the signs, practice defensive computing, and exercise skepticism to avoid having one of these tricks best you.

CURRENT (TECHNOLOGY) AWARENESS

Most of the time if Google or Dropbox or other large provider has a security issue, or goes down for any length of time, the news will make the headlines. At the very least take a quick look at the technology section of the daily news (site/show/program) you consume for any breaking headlines. Legal technology and security blogs, like Sharon Nelson’s Ride the Lightening, or the free daily ABA Journal email are also fantastic resources for the current thought on “is it secure enough for a lawyer?”. Technology, technology companies, terms and conditions, privacy policies, and services are in a constant state of motion. For those products/services you use keep an eye on their press releases, social media outlets, and blogs for information you may need to know.

SECURITY BREACH LEGISLATION

The potential for a security breach is very real. In addition to the ethical obligation of maintaining a client’s confidentiality, you may have a legislative obligation to notify clients if a data breach occurs. More than 543 million records of U.S. residents have been exposed due to security breaches since between January 2005 and December 2011, according to Privacy Rights Clearinghouse, a nonprofit consumer information and advocacy organization. In 2013 alone major companies including Adobe, Target, and the Department of Homeland Security had breaches. A company’s vendors can be a source of such security breaches, as some of the publicized security breaches confirm.

Most law firms, like other businesses, are, subject to two key legal obligations:

- A duty to provide reasonable security for their data and information systems
- A duty to disclose security breaches to those who may be adversely affected by such breaches.

As of January 2014 forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted laws mandating consumer notifications if there is a theft of personal data from the company computers that can be used by thieves to perpetrate identity theft. See the National Conference of State Legislatures’ State Security Breach Notification Laws website and check your state/jurisdiction to determine if the states in which you are licensed have the security breach notification law. The Federal Trade Commission has also brought enforcement actions against companies for not properly protecting sensitive personal data.
In terms of cloud computing and data breach notification the question becomes - if your cloud storage company is breached do you have to notify the client? For instance, if you sync all of your client documents to Google Drive and you read that Google has been hacked do you need to proactively determine whether your account was compromised? If you receive notification that indeed your username and password for your Google account have been compromised do you need to do anything other than change your username and password? For data at rest on a local device many of the data breach notification laws provide that notification is not necessary if the drive is encrypted. Bottom line is that it would be better not to have to ponder the “what if’s”. If you are storing client files with PI (personal information as defined by statute) in the cloud use a third party encryption tool such as BoxCryptor, Viivo, or Sookasa to encrypt the data prior to sending it to the cloud storage. If you store personal information in an online database, like a practice management SaaS for instance, then you need to be clear on how the data is encrypted, who has access to it, and if you will be notified if the data is compromised.

SECURITY POLICIES

Like a medieval castle, your office is your fortress. Multiple walls are needed to keep intruders out, and additional precautions are needed to protect the King from internal dangers. In fact, some studies show that more techno-dangers come from within a business than from the outside.

Information security does not have a one product, one-size-fits-all solution. Hackers and other criminals target some high-profile firms, because of the nature of their work, while others firms go unnoticed. While there may be danger in the cloud, an end users’ compromised system providing a direct path to files stored in Dropbox unbeknownst to the firm, could wreak havoc.

The first line of defense is to have an Internet usage policy for the office or firm. Require all lawyers and staff to only open email attachments from reputable sources. Do not allow non-work related attachments to be opened.

Just having antivirus software is not enough. You must download the latest antivirus definitions to ensure the software contains the most up-to-date detection and prevention. Commercial anti-virus software publishers often sell update subscriptions for about $30 per computer per year; enterprise licenses are much cheaper per seat.

Email messages can be a ticking time bomb, and should therefore be treated with great care. Your firm should have a written policy addressing proper use of firm email for business communication by lawyers and support staff; storage and retention of email as a record; security issues including opening attachments, identifying spam and phishing, and other scams; use of firm email for personal communication; and use of other Internet based communication
tools such as instant messaging, blogging, commenting on blogs, social networking, and online chat.

The SANS Institute has a number of [model policies](#) for internet use, email, downloading applications, and much more which were submitted and sanitized from large corporations. They can be copied and rearranged according to a firm’s needs. The ABA Section of Business Law makes a simple [sample email and Internet use policy](#) available on its website.

In addition to policies, it is essential to train lawyers and staff to stay abreast of the latest threats and how to avoid them. The SANS Institute provides free electronic newsletters through their “Securing the Human” project such as the “OUCH!” security email newsletter and [@RISK](#) email that summarizes the three to eight vulnerabilities that matter most each Thursday. Additionally [ComputerWorld Security](#) email newsletters (Security and Virus & Vulnerability Roundup) provide accurate information about threats. Even most metropolitan newspapers will run stories on technology exploits, especially ones for popular social media sites, in the technology section.

**LOOKING FORWARD**

SaaS is an exciting area of technology and especially legal technology. It’s experiencing explosive growth: in just a few short years we’ve gone from one or two SaaS products on the market to dozens across the whole spectrum of software categories. It seems like a safe bet that the trend will continue as lawyers increasingly rely on web technology and look to break out of traditional office structures. Understanding the technology and how it can fit into your practice at this stage in its development can give you an advantage and a real opportunity to grow and strengthen your practice.

Nevertheless, like any developing technology, it must be treated with caution: information is currency in the legal profession, and failing to appropriately safeguard that information can leave to financial and professional harm for both you and your clients.