Lauletta Birnbaum
ATTORNEYS AT LAW
Doing Business Justice.®

RUNNING YOUR LAW FIRM LIKE A BUSINESS

CYBERSECURITY BEST PRACTICES

By: Frank Lauletta, Randy Ford, and Lauren Reap

The proliferation of cloud-based software services allows smaller law firms to procure business tools and services that are comparable to those employed at large firms but (i) without the huge price tag, (ii) without having to install expensive and complicated systems at your office, and (iii) without employing on-staff IT personnel.

With the speed and agility of this ever-evolving technology, however, comes new and continual threats that must be analyzed and considered with regularity to ensure that you are doing everything that is reasonable to help protect client information.

No matter your specific practice area, your clients trust you with a host of confidential and proprietary information from financial, health and other personal information to trade secrets and intellectual property. As our industry and our clients continue to digitalize this information, new threats continue to surface and expose the vulnerabilities of law firms unprepared or unequipped to maintain best practices designed to help prevent cybersecurity risks.

Sound cyber risk management should encompass technology as well as policies and procedures to help prevent loss. Since no plan or methodology is ever 100% secure, especially as the speed in which technology continues to evolve increases, available insurance solutions should also be considered.

Ethical Considerations

When it comes to lawyers using technology, concerns about security and ethical issues arise. The ABA has ruled that cloud computing is ethical so long as lawyers take "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." [i] Many State Bar Associations, including both Pennsylvania and New Jersey, are following suit with ethics opinions and regulations of their own.

The Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility issued a formal opinion, 2011-200 that answered the question, "may an attorney ethically store confidential client material in 'the cloud'" ("PA Opinion 2011-200"). The short answer is "yes" and will be discussed in greater detail throughout this article.

Additionally, New Jersey's Advisory Committee on Professional Ethics addressed the electronic storage of client information and the use of an outside Internet Service Provider (ISP) in the context of the Rules of Professional Conduct, specifically RPC 1.6 regarding confidentiality. Opinion 701, issued in 2006, advised attorneys utilizing such services are required to exercise reasonable care against the possibility of unauthorized access to client information. Reasonable care includes making use of available technology to guard against foreseeable attempts at unauthorized access.[ii]

At a minimum, to protect your clients' data it is required that you take *reasonable* action to both prevent a breach, and in the event a breach should occur, to mitigate the damage. Reasonable care requires:

- technology to guard against reasonably foreseeable threats;
- due diligence of third party's security measures, recovery methods, and disposal methods; and
- you to require that third parties maintain confidentiality.

Securing Email

The most prudent approach to the ethical duty of protecting confidentiality is to have an express

understanding with clients about the nature of communications that will be, and will not be, sent by email or other electronic means and whether or not encryption and other security measures should be utilized.

Email encryption significantly reduces the risk of exposing confidential information during routine transmissions of electronic communication. Email encryption obscures the content of the email in order to prevent people other than the sender and the recipient from reading the content. Encryption is not currently a blanket obligation for attorneys according to the ABA, nor is the use of unencrypted email, by itself, a violation of the Rules of Professional Conduct, in particular Rule 1.6 ("Confidentiality of Information"). [iii] However, there are certain circumstances when dealing with highly sensitive information, such as health records or certain financial information for example, where the client may have an expectation, and thus you an ethical obligation, to employ greater means of security when electronically transmitting such information. For this reason, attorneys should have encryption available for use in appropriate circumstances.

Furthermore, attorneys have an obligation to oversee work they assign to a non-attorney (e.g., email or cloud computing providers) to make reasonable efforts to ensure that the third party's conduct is compatible with his or her professional obligations.

Web-based email products, such as Gmail, Yahoo Mail or Hotmail, as well as cloud-based services such as Google Apps for Business, are convenient and inexpensive tools for lawyers, however, they may pose potential ethical risks to lawyers. For instance, one could argue that your express agreement in Google's terms and conditions to allow Google to scan email and engage in other data harvesting throughout their apps is a violation of ethical rules disallowing an attorney from using privileged client information to its own benefit or the benefit of a third party without the client's informed consent.

For instance, Rule 1.6 of the Pennsylvania Rules of Professional Conduct provides in relevant part, "a lawyer shall not reveal information relating to representation of a client unless the client gives informed consent." Additionally, the same rule provides later that, "a lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Factors used to determine reasonableness include, "the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use)."[iv] Today, email accounts are fairly inexpensive and the terms and conditions for certain paid accounts do not contain the same potentially problematic terms and conditions that come with a free Gmail account. As a result, it would be wise for a lawyer using a Gmail account to review its applicable terms and consider switching to an alternative commercial email account provider such as Microsoft Office365.

While email and other forms of electronic communication have been employed by lawyers and law firms for decades now, cloud based computing is just now becoming more commonplace in law firms, especially smaller ones. Many communication and productivity tools and services may now be obtained and maintained at significantly lower cost over the Web rather than running and maintaining such applications on your own server at your office. The benefits include the ability to access the services and your files from anywhere and at any time as long as you have an Internet connection. Also, maintenance is typically included in the subscription so there is no need to worry about keeping up with updates since they are automatically installed by the provider.

PA Opinion 2011-200, in response to the ethical obligations regarding the use of cloud computing/software,[v] concluded attorneys may utilize this software as long as "reasonable safeguards are employed to ensure that the data is protected from breaches, data loss and other risks." Some of those "reasonable safeguards" are listed below in Table 1.[vi]

Table 1. Reasonable Safeguards (as determined by the Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility)

- Installing a firewall to limit access to the firm's network.
- Implementing electronic audit trail procedures to monitor who is accessing the data.
- Ensuring your third party provider agrees that it does not own the data, will notify you in the event of a breach or if requested to produce your data, will host your data in a specific geographic country.
- Backing up data to allow the firm to restore data that has been lost, corrupted, or accidentally deleted.
- Retrieving your data from a third party provider if it goes out of business or upon a switch in providers.

Mobile Security

The use of mobile devices has changed the way we share and store business information and has led to numerous challenges regarding the accessibility of confidential information to those who seek to exploit it.

Many public Wi-Fi hot spots, including libraries, coffee shops, and airports, aren't secure. This means other people might be able to get onto your system. To protect your information, turn off the auto-connect feature, so you can choose which networks to use. In the event that you do need to access your system in a public setting, consider utilizing a virtual private network (VPN), or creating your own hot spot through your cellular device or a wireless air card (e.g. MiFi). Additionally, if connecting on a public network, only visit sites that have SSL or HTTPS encryption. Otherwise, you could be opening yourself up to an attack. Each of the options above can provide a safer and more secure connection while trying to get some work done.[vii]

Employers should also have the ability to "remote wipe" a mobile device that ends up lost or stolen. For instance, Microsoft's Office365, which offers cloud based email and related applications, allows the administrator to remotely wipe email, calendar entries, and contacts from mobile devices.

Two-Step Verification

In addition to limiting who has access to nonpublic information, certain client engagements may also require more demanding authentication processes. Two-factor authentication puts an extra barrier in the way of someone who wants to access a service such as your email account, cloud provider, or other system that stores confidential data. With two factor verification, a password is not sufficient to gain access. Instead, a second authentication step is required, typically a code sent to your smartphone via SMS message.

Employee Training

The best policies and practices are useless if your employees do not better understand them nor adhere to them meticulously. Statistics show more breaches occur from employee error than an infiltration of your system.

Some of the most reasonable, and practical, data protection measures include requiring employees to encrypt files stored on laptops or data storage devices (USB or thumb drives) and enabling the lock-screen passcode on any mobile device that can be used to access the company's network. Reports show that about 45% of all smartphone owners actually set a passcode on their device even though each device today allows for some level of passcode protection. Additionally, approximately 5.2 million mobile devices were either lost or stolen during the same time period.[viii]

Not all data protection measures are complicated and costly. By educating employees on basic protection practices and keeping up with current security threats, you can mitigate the risk of a breach and keep your (and your clients') data safe.

Printers and Copier Machines

Computers and mobile devices may be front and center on your radar of devices to protect but do not forget about your printers and copiers. Many firms that require the use of high-volume printers often lease their equipment instead of purchasing due to overall cost and maintenance. In most instances, printers and/or copiers have the capacity to store your print and copy jobs in their internal memory banks. This is likely of little concern when the printer or

Table 2. Quick Tips Designed to Help Prevent a Privacy Breach

1. Train employees in cyber security principles.
2. Secure your Wi-Fi networks, and avoid using public networks while accessing confidential information.
3. Encrypt nonpublic information at rest and in transit.
4. Require individual user accounts for each employee.
5. Regularly change passwords and ensure they meet complexity requirements.
6. Timely destroy nonpublic information.

In addition to the listed tips, the Federal Communications Commission (FCC) provides a tool for small businesses that allows you to create and save a custom cybersecurity plan for your firm, choosing from a menu of expert advice to address your specific business needs and concerns. It can be found at www.fcc.gov/cyberplanner.

copier is maintained and protected in your office, but firms should work with their leasing companies to ensure that all such data is wiped from the printer and/or copier prior to it leaving your premises – otherwise, unencrypted confidential and privileged information is walking right out of your door. Wiping or destroying internal memory banks is a relatively easy task for a printer technician to perform and most reputable companies are set up to provide you with a written certification of destruction for you to put in your files.

Cyber Liability Insurance

Many standard professional liability policies do not cover several of the costs associated with a cyberattack including:

- Hiring forensic experts to investigate the breach;
- Restoring and recreating data;
- Notification to clients;
- Addressing regulatory inquiries;
- Fines associated with breach; and
- Business interruption, including lost income.

Insurance for the above risks are instead covered by a separate policy or endorsement called cyber liability insurance. The application process for cyber liability insurance often requires documenting the current cybersecurity practices in place, and can point out deficiencies and offer a road map moving forward. Data encryption, mobile security and employee training are pieces of a multi-part solution for cybersecurity.

An effective cyber liability policy should first and foremost be a primary policy, and should cover a breach of anything protected under attorney-client privilege, not just personally identifiable information. It is also important to assess any additional services the insurer offers such as remediation benefits that will aid in your response to an incident.

Selecting the proper providers and vendors that have experience in the ethical considerations as well as the risks encountered by law firms is a smart first step. Doing your own research and due diligence with respect to each piece of your technology puzzle is a must since your providers and vendors are likely not lawyers and the obligations owed to your clients ultimately lies with you.

About Lauletta Birnbaum

Lauletta Birnbaum's highly-credentialed, business-minded attorneys provide a range of business, corporate, securities, intellectual property and litigation services to private and publicly held companies in various industries such as software, high technology, energy, telecommunications, manufacturing, media, banking and real estate.

Designed to maximize flexibility and value in this ever-evolving business climate, the firm offers real-world business strategy and legal expertise, often serving as outside general counsel to its clients. Its mission is to help its middle market clients achieve significant legal budget reductions while helping them to increase revenue, all without compromising quality and responsiveness. To learn more, visit Lauletta.com.

[i] See American Bar Association Commission on Ethics 20/20 Working Group on the Implications of New Technologies – "Issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology" – 20 Sept. 2010.

[ii] See New Jersey Advisory Committee on Professional Ethics – "Electronic Storage and Access of Client Files" - Opinion 701 (2006).

[iii] See American Bar Association Standing Commission on Ethics and Professional Responsibility – Formal Opinion 99-413 (1999).
[iv] Rule 1.6, Pennsylvania Rules of Professional Conduct.
[v] See Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility – "Ethical Obligations for Attorneys Using Cloud Computing/Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property" – Formal Opinion 2011-200.
[vi] See Id. Pages 8 -10.
[vii] Stone, Jeff. "How to Protect Yourself on Public Wi-Fi: Free, Open Internet Can be Awesome, But it's a Huge Security Risk." International Business Times. 26 February 2016. Web. 2 February 2017.
[viii] Deitrick, Calla. "Smartphone Thefts Drop as Kill Switch usage Grows." Consumer Reports. 6 June 2015. Web. 2 February 2017.

