Locked Down! Information Security for Lawyers

Sharon D. Nelson, Esq. and John W. Simek
President and Vice President
Sensei Enterprises, Inc.
www.senseient.com
snelson@senseient.com
jsimek@senseient.com
Contents

Introduction ........................................................................................................................ 3
The Threats ......................................................................................................................... 3
Duty to Safeguard ............................................................................................................. 10
1. Ethics Rules ........................................................................................................... 11
2. Ethics Opinions ...................................................................................................... 13
3. Ethics Rules – Electronic Communications ........................................................ 15
4. Ethics Opinions – Electronic Communications ...................................................... 16
5. Common Law Duties ............................................................................................. 18
6. Laws and Regulations Covering Personal Information .......................................... 18
7. Summary of Duties ................................................................................................ 20
Information Security Basics .............................................................................................. 21
Reasonable Safeguards ..................................................................................................... 22
Conclusion ......................................................................................................................... 24
Additional Information ......................................................................................................... 24
Introduction

Confidential data in computers and information systems, including those used by attorneys and law firms, faces greater security threats today than ever before. They take a variety of forms, ranging from e-mail phishing scams and social engineering attacks to sophisticated technical exploits resulting in long term intrusions into law firm networks. They also include inside threats, from malicious, to untrained, to inattentive personnel. These threats are a particular concern to attorneys because of their duty of confidentiality. Attorneys have ethical and common law duties to take competent and reasonable measures to safeguard information relating to clients. They also often have contractual and regulatory duties to protect client information and other types of confidential information.

Effective information security requires an ongoing, comprehensive process that addresses people, policies and procedures, and technology. It also requires an understanding that security is everyone’s responsibility and constant security awareness by all users of technology.

The Threats

For years, technology attorneys and information security professionals warned lawyers that it was not a question of whether law firms would become victims of successful hacking attacks - it was a matter of when. They pointed to numerous law firm incidents of dishonest insiders and lost or stolen laptops and portable media, but there were not disclosed incidents of successful hacking attacks. It has now reached the “when” – over the last several years, there have been increasing reports in the popular, legal, and security media of successful attacks on attorneys and law firms. They have occurred and are occurring - and attorneys and law firms need to comprehensively address security.

A December 2009 FBI alert warned that law firms and public relations firms were being targeted with spear phishing e-mails containing malicious payloads. In January 2010, the FBI issued

---

1 Parts of this paper are adapted from prior materials prepared by the author, including David G. Ries, “Safeguarding Confidential Data: Your Ethical and Legal Obligations,” Law Practice (July/August 2010) and David G. Ries, “Cybersecurity for Attorneys: Understanding the Ethical Obligations,” Law Practice TODAY (March 2012).

2 “Spear phishing” is fraudulent e-mail that falsely appears to be from a trusted source and targets a specific organization or individual, seeking unauthorized access to confidential data.

another alert, this time warning law firms about counterfeit check schemes that used e-mails to lure them into relationships with fraudulent overseas “clients.”

The news reports started with a February, 2010, *Wired Magazine* article that reported on advanced persistent threats (APTs), a particularly nasty form of coordinated and extended hacking attack. It discussed an example of a 2008 APT attack on a law firm that was representing a client in Chinese litigation:

> The attackers were in the firm’s network for a year before the firm learned from law enforcement that it had been hacked. By then, the intruders harvested thousands of e-mails and attachments from mail servers. They also had access to every other server, desktop workstation and laptop on the firm’s network.

This attack was investigated by Mandiant, a leading information security firm that specializes in investigation of data breaches. Mandiant discovered that the network had been breached for more than a year before the law firm was tipped off to the breach by law enforcement. They could not determine the initial attack vector because the law firm did not have system logs available. The intruders at the law firm were able to obtain more than 30 sets of user credentials, compromise approximately three dozen workstations, and gain full access to all servers and computers on the network for an extended time.

A *National Law Journal* article in March, 2010, reported that Mandiant assisted over 50 law firms after security breaches. A Mandiant forensics specialist stated in an interview that Mandiant spent approximately 10% of its time in 2010 investigating data breaches at law firms.

The same month, an article in the *San Francisco Chronicle*, “Law Firms Are Lucrative Targets of Cyberscams,” discussed recent attacks on attorneys, ranging from phishing scams to intrusions into law firm networks to steal lawsuit-related information. It reported:

> Security experts said criminals gain access into law firms’ networks using highly tailored schemes to trick attorneys into downloading customized malware into their computers. It is not uncommon for them to remain undetected for long periods of time and come and go as they please, they said.

---

6 See Mandiant’s *M-Trends [the advanced persistent threat] (2010).*
In November, 2011, the FBI held a meeting for the 200 largest law firms in New York to advise them about the increasing number of attacks. *Bloomberg News* reported:  

> Over snacks in a large meeting room, the FBI issued a warning to the lawyers: Hackers see attorneys as a back door to the valuable data of their corporate clients.

> “We told them they need a diagram of their network; they need to know how computer logs are kept,” Galligan [the head of the FBI cyber division in New York City] said of the meeting. “Some were really well prepared; others didn’t know what we were talking about.”

Successful attacks on law firms have continued. *Bloomberg News* published “China-Based Hackers Target Law Firms to Get Secret Deal Data” in January, 2012.  

> It described a group of major hacking incidents in which attackers successfully targeted 7 Canadian law firms and 2 Canadian government agencies to get information about a transaction involving the sale of potash mines in Western Canada. The article reports that Mandiant estimated that 80 major law firms were hacked during 2011.

The SANS Institute, a highly regarded information security research, education, and certification organization, has published an interview with the managing partner and IT partner of a New York law firm that had been hacked. The attorneys said that the FBI told the law firm that “our files had been found on a server in another country. The server was used as a way station for sending data to a large Asian country.”

Effective information security is now a requirement for attorneys. In June, 2012, the *Wall Street Journal* published “Client Secrets at Risk as Hackers Target Law Firms.” It started with:

> Think knowing how to draft a contract, file a motion on time and keep your mouth shut fulfills your lawyerly obligations of competence and confidentiality?

> Not these days. Cyberattacks against law firms are on the rise, and that means attorneys who want to protect their clients’ secrets are having to reboot their skills for the digital age.

---


11 Id.

12 SANS Institute, “Conversations About Cybersecurity.”  
www.sans.org/security-resources/cybersecurity-conversations.
Security threats to law firms continue to grow. In February, 2013, an FBI agent gave a keynote presentation on law firm security threats at LegalTech New York. In an article reporting on it, the special agent in charge of the FBI’s cyber operations in New York City is quoted as stating:13

“We have hundreds of law firms that we see increasingly being targeted by hackers. …We all understand that the cyberthreat is our next great challenge. Cyber intrusions are all over the place, they’re dangerous, and they’re much more sophisticated” than they were just a few years ago.

In August, 2013, ILTA (the International Legal Technology Association) presented "The FBI and Experts Present Security Updates and Strategies for Firms of All Sizes" at its Annual Conference. An FBI speaker called it “a paradigm shift” and noted that attackers are “already in the system.” Another speaker observed that several practice areas appear to be most vulnerable to attack, including oil and gas, technology, and technology patents.14

Last year, Shane McGee, the general counsel and vice president of legal affairs at Mandiant Corp., is quoted in a September, 2013 ABA Journal article as follows:15

Law firms need to understand that they’re being targeted by the best, most advanced attackers out there … These attackers will use every resource at their disposal to compromise law firms because they can, if successful, steal the intellectual property and corporate secrets of not just a single company but of the hundreds or thousands of companies that the targeted law firm represents. Law firms are, in that sense, ‘one-stop shops’ for attackers.

The information on these law firm data breaches is consistent with breaches generally - many are found by third-parties and many are discovered after an extended time. The Verizon 2013 Data Breach Investigation Report, reporting on data breaches in 2012 generally, reports that 70% were discovered by a third party and 66% were detected after months or years.16

While the large scale hacking attacks make attention-grabbing headlines, law firms also continue to face smaller scale, yet still serious, security incidents, like lost or stolen laptops, tablets, smartphones, and USB drives. For example, a Maryland law firm lost an unencrypted portable

---

hard drive containing medical information when an employee left it on a light rail train. The idea was good – take it offsite for backup – but the execution was a security risk – it wasn’t encrypted.

It happened again in June, 2014. A Georgia-based criminal defense firm reported that a backup drive containing personal information, including Social Security numbers, was stolen from an employee’s locked trunk. It was not encrypted.

In addition to threats from criminals and hackers, law firms, like other businesses and enterprises, also face threats from the inside. The insider threat includes a spectrum of trusted employees and third-parties with access, ranging from criminal, to malicious, to disgruntled, to untrained, to careless, to bored, to honestly mistaken. It even includes dedicated employees who just want to use their own technology to do their jobs better. Unauthorized hardware, software, and services can be a threat from insiders in any of these groups. A recent international survey of IT security professionals reported that 41% of those surveyed viewed rogue employees as the biggest threats to their organizations.

A recent survey reported the following on the scope of the risk from employee use of their own technology:

> It's out there: lurking in cubicles, infiltrating boardrooms, pulsing through desktops and laptops and tablets. Viral. Relentless. Unstoppable.

Rogue IT is the name given to the informal, ad hoc software and devices brought by employees into the workplace. If you've ever taken your own iPad to work or used cloud-based software like Evernote or Dropbox in the office, you may well be an offender. And you're not alone. Some 43% of businesses report that their employees are using cloud services independently of the IT department, according to a recent survey of 500 IT decision makers.

A recognized security consultant has summarized the accidental insider threat this way:

---


Much is misunderstood today about the evolving insider threat. …In particular, senior leaders need to realize that their greatest risks aren’t from rogue employees looking to cause damage, but rather from inadvertent breaches caused by staffers who simply stumble into costly mistakes.

The FBI’s Chief Information Security Officer expressed the same concern in a presentation on the FBI’s insider threat program at the 2013 RSA Security Conference. The FBI’s program was created after the 2001 Robert Hanssen incident in which an FBI agent was caught stealing information and selling it to the Russians. The CISO noted that authorized users with a level of organizational trust, who are doing legitimate activities with malicious intent, pose the biggest threat. But a quarter of the incidents that the FBI tracks in its systems on an annual basis are from "knucklehead" problems: unintentional acts in which employees compromise systems by not following procedures, losing equipment and sensitive data, clicking on spam, inappropriate emails or Web links, or mishandling passwords and accounts. He said the FBI spends about 35% of its response time on these types of incidents.

Insider security incidents are often not publicly disclosed unless they lead to criminal prosecution or required data breach notices. For this reason, the availability of statistics and examples is limited. The incident of the hard drive left on the light rail is an example of the insider threat in a law firm – most likely from a lack of security procedures, inadequate training, or both.

There are also older examples of intentional insider threats in law firms that illustrate the risks. A former Manhattan paralegal was sentenced to prison after pleading guilty to downloading his firm’s 400 page electronic trial plan for an asbestos case and offering to sell it to opposing counsel. In another example, a college student who worked for a service provider at a law firm pled guilty to theft of intellectual property. The student was brought in to help by his uncle, an employee of the service provider, because they were behind on the job. The firm represented DirecTV in litigation with one of its security vendors. The student worked in a secure area in the law firm’s offices, where he copied paper and electronic data for production in the litigation. He found the technology that controlled access by customers to DirecTV, copied it to a CD, and posted it on a hacker bulletin board. In a third example, a former IT employee of a large law firm pled guilty to theft of 156 computers and monitors from the law firm that he sold on eBay for over

---


$74,000. More recently, a Pennsylvania law firm sued a former attorney, alleging that he took thousands of client files using Dropbox.

As these examples of security incidents of all kinds demonstrate, law firm data faces substantial and real threats. The American Bar Association’s 2014 Technology Survey reports that 13.8% of all responding attorneys reported that their firm had suffered a security breach at some time, broken down by size of firm as follows:

<table>
<thead>
<tr>
<th>Size of Firm</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solo</td>
<td>11.7%</td>
</tr>
<tr>
<td>2-9</td>
<td>13.3%</td>
</tr>
<tr>
<td>10-49</td>
<td>18.8%</td>
</tr>
<tr>
<td>50-99</td>
<td>15.0%</td>
</tr>
<tr>
<td>100-499</td>
<td>9.5%</td>
</tr>
<tr>
<td>500 or More</td>
<td>17.2%</td>
</tr>
<tr>
<td>All Firms</td>
<td>13.8%</td>
</tr>
</tbody>
</table>

A number of responding attorneys reported that they didn’t know whether their firm had suffered a security breach in the past – 67.2% of large firms and 25.7% of all firms.

In addition to these other growing threats, a current concern for security and confidentiality for attorneys, particularly those representing foreign clients or engaged in international transactions, is government surveillance – both by the U.S. government and foreign governments. In August of 2013, the ABA adopted a resolution, recommended by the ABA Cybersecurity Legal Task Force, condemning intrusions into attorneys’ systems and networks, including those by governments.

It included the following:

RESOLVED, That the American Bar Association condemns unauthorized, illegal governmental, organizational and individual intrusions into the computer systems and networks utilized by lawyers and law firms.

In February of 2014, the New York Times reported that documents leaked by Edward Snowden showed that an American law firm had been monitored by the Australian Signals Directorate, an

---


27 Available at www.americanbar.org/content/dam/aba/administrative/law_national_security/resolution_118.authcheckdam.pdf
NSA ally, while the law firm was representing a foreign government in trade disputes with the U.S. Following this report, ABA President James Silkenat wrote to the Director and General Counsel of the NSA about this incident, including:

I write to express our concerns over allegations raised in recent press reports concerning possible foreign government surveillance of American lawyers’ confidential communications with their overseas clients, the subsequent sharing of privileged information from those communications with the National Security Agency (“NSA”), and the possible use of that information by the U.S. Government or third parties.”

NSA Director, General Keith Alexander, responded, noting:

NSA is firmly committed to the rule of law and the bedrock legal principle of attorney-client privilege, which as you noted, is one of the oldest recognized privileges for confidential communications.

***

Let me be absolutely clear: NSA has afforded, and will continue to afford, appropriate protection to privileged attorney-client communications acquired during its lawful foreign intelligence mission in accordance with privacy procedures required by Congress, approved by the Attorney General, and, as appropriate, reviewed by the Foreign Intelligence Surveillance Court.”

Security threats to lawyers and law firms continue to be substantial, real, and growing – data breaches and security incidents have occurred and are occurring. It is critical for attorneys and law firms to recognize them and address them through comprehensive information security programs.

**Duty to Safeguard**

Attorneys’ use of technology presents special ethics challenges, particularly in the areas of competence and confidentiality. Attorneys also have common law duties to protect client information and may have contractual and regulatory duties. These duties to safeguard information relating to clients are minimum standards with which attorneys are required to comply. Attorneys should aim for even stronger safeguards as a matter of sound professional practice and client service.

---


1. **Ethics Rules**

The duty of competence (ABA Model Rule 1.1) requires attorneys to know what technology is necessary and how to use it. The duty of confidentiality (ABA Model Rule 1.6) is one of an attorney’s most fundamental ethical responsibilities. Together, these rules require attorneys using technology to take competent and reasonable measures to safeguard client data. This duty extends to all use of technology, including computers, mobile devices, networks, technology outsourcing, and cloud computing.

Model Rule 1.1 covers the general duty of competence. It provides that “A lawyer shall provide competent representation to a client.” This “requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.” It includes competence in selecting and using technology. It requires attorneys who lack the necessary technical competence for security (many, if not most attorneys) to consult with qualified people who have the requisite expertise.

Model Rule 1.4, Communications, also applies to attorneys’ use of technology. It requires appropriate communications with clients “about the means by which the client’s objectives are to be accomplished,” including the use of technology. It requires keeping the client informed and, depending on the circumstances, may require obtaining “informed consent.” It requires notice to a client of compromise of confidential information relating to the client.

Model Rule 1.6 generally defines the duty of confidentiality. It begins as follows:

> A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b). . . .

Rule 1.6 broadly requires protection of “information relating to the representation of a client;” it is not limited to confidential communications and privileged information. Disclosure of covered information generally requires express or implied client consent (in the absence of special circumstances like misconduct by the client).

The ABA Commission on Ethics 20/20 conducted a review of the ABA Model Rules of Professional Conduct and the U.S. system of lawyer regulation in the context of advances in technology and global legal practice developments. One of its core areas of focus was technology and confidentiality. Its Revised Draft Resolutions in this area were adopted by the ABA at its Annual Meeting in August of 2012.31

The amendments include addition of the following highlighted language to the Comment to Model Rule 1.1 Competence:

> [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 technology, . . .

31 See, [www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20.html](http://www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20.html).
The amendments also added the following new subsection (highlighted) to Model Rule 1.6
Confidentiality of Information:

(c) 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.

This requirement covers two areas – inadvertent disclosure and unauthorized access. Inadvertent disclosure includes threats like leaving a briefcase, laptop, or smartphone in a taxi or restaurant, sending a confidential e-mail to the wrong recipient, producing privileged documents or data, or exposing confidential metadata. Unauthorized access includes threats like hackers, criminals, malware, and insider threats.

The amendments also include the following changes to Comment [18] to this rule:

**Acting Competently to Preserve Confidentiality**

[18] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons or entities who are participating in the representation of the client or who are subject to the lawyer’s supervision or monitoring. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, confidential information does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer’s efforts 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). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forego 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.

Significantly, these revisions are clarifications rather than substantive changes. They add additional detail that is consistent with the then existing rules and comments, ethics opinions, and generally accepted information security principles.32

---

32 “This duty is already described in several existing Comments, but the Commission concluded that, in light of the pervasive use of technology to store and transmit confidential client information, this existing obligation should be stated explicitly in the black letter of Model Rule 1.6.” ABA Commission on Ethics 20/20, *Report to Resolution 105A Revised*, Introduction (2012).
Model Rule 5.3 (Responsibilities Regarding Nonlawyer Assistants) was amended to expand its scope. “Assistants” was expanded to “Assistance,” extending its coverage to all levels of staff and outsourced services ranging from copying services to outsourced legal services. This requires attorneys to employ reasonable safeguards, like due diligence, contractual requirements, supervision, and monitoring, to insure that nonlawyers inside and outside a law firm provide services in compliance with attorneys’ duty of confidentiality.

2. Ethics Opinions

A number of state ethics opinions have addressed professional responsibility issues related to security in attorneys’ use of various technologies. Consistent with the subsequent Ethics 20/20 amendments, they generally require competent and reasonable safeguards. It is important for attorneys to consult the rules, comments, and ethics opinions in the relevant jurisdiction(s).

An early example is State Bar of Arizona, Opinion No. 05-04 (July 2005) (Formal Opinion of the Committee on the Rules of Professional Conduct). It requires “competent and reasonable steps to assure that the client’s confidences are not disclosed to third parties through theft or inadvertence” and “competent and reasonable measures to assure that the client’s electronic information is not lost or destroyed.” It further explains that “an attorney must either have the competence to evaluate the nature of the potential threat to the client’s electronic files and to evaluate and deploy appropriate computer hardware and software to accomplish that end, or if the attorney lacks or cannot reasonably obtain that competence, to retain an expert consultant who does have such competence.”

Additional examples include New Jersey Advisory Committee on Professional Ethics, Opinion 701, “Electronic Storage and Access of Client Files” (April, 2006), State Bar of Arizona, Opinion No. 09-04 (December, 2009): “Confidentiality; Maintaining Client Files; Electronic Storage; Internet” (Formal Opinion of the Committee on the Rules of Professional Conduct); and State Bar of California, Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2010-179.

Significantly, California Formal Opinion No. 2010-179 advises attorneys that they must consider security before using a particular technology in the course of representing a client. It notes that attorneys “must take appropriate steps to evaluate,” among other considerations, “the level of security attendant to the use of that technology, including whether reasonable precautions may be taken when using the technology to increase the level of security.” The opinion covers use of a firm-issued laptop and use of public and home wireless networks.

Attorneys need to stay up to date as technology changes and new threats are identified. For example, following news reports that confidential information had been found on digital copiers that were ready for resale,33 The Florida Bar issued Professional Ethics of the Florida Bar Opinion 10-2 (September, 2010) that addresses this risk. Its conclusion states:

In conclusion, when a lawyer chooses to use Devices that contain Storage Media, the lawyer must take reasonable steps to ensure that client confidentiality is maintained and that the Device is sanitized before disposition. These reasonable steps include: (1) identification of the potential threat to confidentiality along with the development and implementation of policies to address the potential threat to confidentiality; (2) inventory of the Devices that contain Hard Drives or other Storage Media; (3) supervision of nonlawyers to obtain adequate assurances that confidentiality will be maintained; and (4) responsibility for sanitization of the Device by requiring meaningful assurances from the vendor at the intake of the Device and confirmation or certification of the sanitization at the disposition of the Device.

There are now multiple ethics opinions on attorneys’ use of cloud computing services like online file storage and software as a service (SaaS).\textsuperscript{34} For example, New York Bar Association Committee on Professional Ethics Opinion 842 “Using an outside online storage provider to store client confidential information” (September, 2010), consistent with the general requirements of the ethics opinions above, concludes:

A lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality is maintained in a manner consistent with the lawyer's obligations under Rule 1.6. A lawyer using an online storage provider should take reasonable care to protect confidential information, and should exercise reasonable care to prevent others whose services are utilized by the lawyer from disclosing or using confidential information of a client. In addition, the lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client's information, and the lawyer should monitor the changing law of privilege to ensure that storing information in the "cloud" will not waive or jeopardize any privilege protecting the information.


The key professional responsibility requirements from these various opinions on attorneys’ use of technology are \textit{competent and reasonable measures to safeguard client data}, including an understanding of limitations in attorneys’ competence, obtaining appropriate assistance,

\textsuperscript{34} The ABA Legal Technology Resource Center has published a summary with links, “Cloud Ethics Opinions Around the U.S.,” available at www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html.
continuing security awareness, appropriate supervision, and ongoing review as technology, threats, and available security evolve.

3. **Ethics Rules – Electronic Communications**

E-mail and electronic communications have become everyday communications forms for attorneys and other professionals. They are fast, convenient, and inexpensive, but also present serious risks. It is important for attorneys to understand and address these risks.

In addition to adding the requirement of reasonable safeguards to protect confidentiality, the Ethics 2000 revisions to the Model Rules, over 10 years ago, also added Comment 17 [now 19] to Rule 1.6. This comment requires reasonable precautions to safeguard and preserve confidential information during electronic transmission. This Comment, as amended in accordance with the Ethics 20/20 recommendations (highlighted), provides:

> [19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer’s expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

This Comment requires attorneys to take “reasonable precautions” to protect the confidentiality of electronic communications. It is often viewed as providing that attorneys never need to use “special security measures” like encryption. While it does state that “special security measures” are not generally required, it contains qualifications and notes that “special circumstances” may warrant “special precautions.” It includes the important

---

35 Encryption is a process that translates a message into a protected electronic code. The recipient (or anyone intercepting the message) must have a key to decrypt it and make it readable. E-mail encryption has become easier to use over time. Transport layer security (TLS) encryption is available to automatically encrypt e-mail between two e-mail gateways. If a law firm and client each have their own e-mail gateways, TLS can be used to automatically encrypt all e-mails between them. A virtual private network is an arrangement in which all communications between two networks or between a computer and a network are automatically protected with encryption. See, David G. Ries and John W. Simek, “Encryption Made Simple for Lawyers,” GPSolo Magazine (November/December 2012).
qualification - “if the method of communication affords a reasonable expectation of privacy.” As discussed below, there are questions about whether Internet e-mail affords a reasonable expectation of privacy.

4. Ethics Opinions – Electronic Communications

An ABA ethics opinion in 1999 and several state ethics opinions have concluded that special security measures, like encryption, are not generally required for confidential attorney e-mail. However, these opinions should be carefully reviewed because, like Comment 19, they contain qualifications that limit their general conclusions.

For example, New York Bar Association Committee on Professional Ethics Opinion 709 “Use of Internet to advertise and to conduct law practice focusing on trademarks; use of Internet e-mail; use of trade names” (September, 1998) concludes:

We therefore conclude that lawyers may in ordinary circumstances utilize unencrypted Internet e-mail to transmit confidential information without breaching their duties of confidentiality … to their clients, as the technology is in use today. Despite this general conclusion, lawyers must always act reasonably in choosing to use e-mail for confidential communications, as with any other means of communication. Thus, in circumstances in which a lawyer is on notice for a specific reason that a particular e-mail transmission is at heightened risk of interception, or where the confidential information at issue is of such an extraordinarily sensitive nature that it is reasonable to use only a means of communication that is completely under the lawyer's control, the lawyer must select a more secure means of communication than unencrypted Internet e-mail.

A lawyer who uses Internet e-mail must also stay abreast of this evolving technology to assess any changes in the likelihood of interception as well as the availability of improved technologies that may reduce such risks at reasonable cost. It is also sensible for lawyers to discuss with clients the risks inherent in the use of Internet e-mail, and lawyers should abide by the clients’ wishes as to its use.

36 E.g., ABA Formal Opinion No. 99-413, Protecting the Confidentiality of Unencrypted E-Mail (March 10, 1999) (“based upon current technology and law as we are informed of it …a lawyer sending confidential client information by unencrypted e-mail does not violate Model Rule 1.6(a)…” “…this opinion does not, however, diminish a lawyer's obligation to consider with her client the sensitivity of the communication, the costs of its disclosure, and the relative security of the contemplated medium of communication. Particularly strong protective measures are warranted to guard against the disclosure of highly sensitive matters.”) and District of Columbia Bar Opinion 281, “Transmission of Confidential Information by Electronic Mail,” (February, 1998), (“In most circumstances, transmission of confidential information by unencrypted electronic mail does not per se violate the confidentiality rules of the legal profession. However, individual circumstances may require greater means of security.”).
There are serious questions about the confidentiality of Internet e-mail. Respected security professionals for years have compared e-mail to postcards or postcards written in pencil. A June 2014 post by Google on the Google Official Blog and a July 2014 New York Times article use the same analogy – comparing unencrypted e-mails to postcards. Encryption is being increasingly required in areas like banking and health care. New laws in Nevada and Massachusetts (which apply to attorneys as well as others) require defined personal information to be encrypted when it is electronically transmitted. As the use of encryption grows in areas like these, it will become difficult for attorneys to demonstrate that confidential client data needs lesser protection. Consistent with these questions about the security of e-mail, some ethics opinions express a stronger view that encryption may be required. For example, New Jersey Opinion 701 (April, 2006), discussed above, notes at the end: “where a document is transmitted to [the attorney]… by email over the Internet, the lawyer should password a confidential document (as is now possible in all common electronic formats, including PDF), since it is not possible to secure the Internet itself against third party access.”

California Formal Opinion No. 2010-179, also discussed above, notes that “encrypting email may be a reasonable step for an attorney in an effort to ensure the confidentiality of such


38 “Transparency Report: Protecting Emails as They Travel Across the Web,” Google Official Blog (June 3, 2014) (“…we send important messages in sealed envelopes, rather than on postcards. …Email works in a similar way. Emails that are encrypted as they’re routed from sender to receiver are like sealed envelopes, and less vulnerable to snooping—whether by bad actors or through government surveillance—than postcards.”)


39 Molly Wood, “Easier Ways to Protect Email From Unwanted Prying Eyes,” New York Times (July 16, 2014) (“Security experts say email is a lot more like a postcard than a letter inside an envelope, and almost anyone can read it while the note is in transit. The government can probably read your email, as can hackers and your employer.”)


41 Mass. Gen. Laws Ch. 93H, regulations at 201 CMR 17.00.

42 File password protection in some software, like current versions of Microsoft Office, Adobe Acrobat, and WinZip uses encryption to protect security. It is generally easier to use than encryption of e-mail and attachments. However, the protection can be limited by use of weak passwords that are easy to break or “crack.”
communications remain so when circumstances call for it, particularly if the information at issue is highly sensitive and the use of encryption is not onerous.”

An Iowa opinion on cloud computing suggests the following as one of a series of questions that attorneys should ask when determining appropriate protection: “Recognizing that some data will require a higher degree of protection than others, will I have the ability to encrypt certain data using higher level encryption tools of my choosing?” Iowa Ethics Opinion 11-01.

The recent Pennsylvania ethics opinion on cloud computing, discussed above, concludes that “attorneys may use email but must, under appropriate circumstances, take additional precautions to assure client confidentiality.” It discusses encryption as an additional precaution that may be required when using services like web mail. Pennsylvania Formal Opinion 2011-200.

In addition to complying with any legal requirements that apply, 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 electronically and whether or not encryption and other security measures will be utilized.

It has now reached the point (or at least is reaching it) where most attorneys should have encryption available for use in appropriate circumstances.

5. Common Law Duties

Along with these ethical duties, there are also parallel common law duties defined by case law in the various states. The Restatement (3rd) of the Law Governing Lawyers (2000) summarizes this area of the law. See, Section 16(2) on competence and diligence, Section 16(3) on complying with obligations concerning client’s confidences, and Chapter 5, “Confidential Client Information.” Breach of these duties can result in a malpractice action.

There are also instances when lawyers have contractual duties to protect client data. This is particularly the case for clients in regulated industries, such as health care and financial services, that have regulatory requirements to protect privacy and security. Clients are recognizing that law firms may be the weak links in protecting their confidential information and are increasingly requiring specified safeguards, providing questionnaires about a law firm’s security, and even requiring security audits.43

6. Laws and Regulations Covering Personal Information

In addition to the ethical and common law duties to protect client information, various state and federal statutes and regulations require protection of defined categories of personal information. Some of these are likely to apply to lawyers who possess any specified personal information about their employees, clients, clients’ employees or customers, opposing parties and their employees, or even witnesses.

At least 10 states now have general security laws that require reasonable measures to protect defined categories of personal information (including California, Massachusetts, Maryland, New Jersey and Rhode Island). While the scope of coverage, the specificity of the requirements and the definitions vary among these laws, personal information is usually defined to include general or specific facts about an identifiable individual. The exceptions tend to be information that is presumed public and does not have to be protected (e.g., a business address).

There are now a number of state laws that require specific safeguards for defined types of personal information as well. They generally cover Social Security numbers, driver’s license numbers and financial account numbers, but some also cover health information. They include laws requiring reasonable security, breach notices and secure disposal.

The most comprehensive law of this type to date is a recent Massachusetts law, M.G.L. c. 93H, which applies to “persons who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts.” Covered “personal information” includes Social Security numbers, driver’s license numbers, state-issued identification card numbers, financial account numbers and credit card numbers.

The implementing regulation became effective March 1, 2010. With its broad coverage of “persons,” this law may well be applied to persons nationwide, including attorneys and law firms, when they have sufficient contacts with Massachusetts to satisfy personal jurisdiction requirements.

It requires covered persons to “develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards.” In addition to requiring a risk assessment, the regulation contains detailed requirements for the information security program and detailed computer system security requirements. The security requirements include:

- Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly; and
- Encryption of all personal information stored on laptops or other portable devices.

Additional system security requirements are secure user authentication, secure access control, reasonable monitoring to detect unauthorized access, reasonably up-to-date firewall protection, reasonably up-to-date security software (including current patches and virus definitions), and education and training of employees.

Lawyers and law firms should think about and understand the consequences of the Massachusetts law, as some observers believe that it will become a model for comprehensive protection of personal information.
Nevada also has laws that require “reasonable security measures” and encryption (NRS 603A.210 and NRS 597.970), although they are much less detailed than the Massachusetts law. Note, too, that encryption is already required for federal agencies that have information about individuals on laptops and portable media. As encryption becomes a security standard, it is likely to become the standard of what is reasonable for lawyers.

The obligations don’t stop, however, at protecting the confidentiality of information. Forty-seven states and the District of Columbia and the Virgin Islands have laws that require notification concerning data breaches (all but Mississippi, New Mexico and South Dakota). While there are differences in their scope and requirements, they generally require entities that own, license or possess defined categories of personally identifiable information about consumers to notify affected consumers if there is a breach. Like the reasonable security laws, many of these laws apply to covered information “about” residents of the state. Some require notice to a state agency in addition to notice to consumers.

In addition to these state laws, a number of bills have been introduced in Congress during the last several years to set minimum federal standards for protection of personal information and breach notice. While there appears to be strong support for a federal solution, nothing has been enacted because of factors like disagreement about details of a solution and overlapping committee jurisdiction. Following the recent high profile Target data breach, legislation has again been introduced, with requirements like requiring the Federal Trade Commission (FTC) to issue security standards for companies that hold consumers’ personal and financial information and setting uniform federal standards for breach notification. For example, several Senators introduced the Personal Data Privacy and Security Act, the fourth time it was introduced since 2005, others introduced the Data Security and Breach Notification Act, and another group introduced the Personal Data Protection and Breach Accountability Act.

To add to the web of issues involved, at least 19 states also now have laws that require secure disposal of paper and electronic records that contain defined personal information. The Federal Trade Commission’s Disposal Rule, 16 C.F.R. Part 682, has similar requirements for consumer credit reports and information derived from them.

Also on the federal level, an attorney who receives protected individually identifiable health information (PHI) from a covered entity under the Health Insurance Portability & Accountability Act (HIPAA) will generally be a “business associate” and be required to comply with the HIPAA security requirements. The 2009 HIGHTECH Act enhanced HIPAA security requirements, extended them directly to business associates, and added a new breach notification requirement. See, 45 CFR Parts 160 and 164.

7. Summary of Duties

The ethics rules and common law duties require attorneys to take competent and reasonable measures to safeguard client data, including an understanding of limitations in attorneys’ competence, obtaining appropriate assistance, continuing security awareness, appropriate supervision, and ongoing review as technology, threats, and available security evolve. These ethical and common law duties, as well as any applicable contractual and regulatory duties, are minimum standards of conduct. Attorneys should aim for even stronger safeguards as a matter of sound professional practice and client service. While the risks of
disciplinary proceedings, malpractice claims, and regulatory actions arising from security breaches are real, the greatest risks are often dissatisfied clients (or former clients) and harm to professional reputation.

**Information Security Basics**

Information security is a process to protect the confidentiality, integrity, and availability of information. Comprehensive security must address people, policies and procedures, and technology. While technology is a critical component of effective security, the other aspects must also be addressed. As explained by Bruce Schneier, a highly respected security professional, "[i]f you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology." The best technical security is likely to fail without adequate attention to people and policies and procedures. Many attorneys incorrectly think that security is just for the IT department or consultants. While IT has a critical role, everyone, including management, all attorneys, and all support personnel, must be involved for effective security.

An equally important concept is that security requires training and ongoing attention. It must go beyond a onetime “set it and forget it” approach. A critical component of a law firm security program is constant vigilance and security awareness by all users of technology. As a recent ABA report aptly put it:

> Lawyers must commit to understanding the security threats that they face, they must educate themselves about the best practices to address those threats, and they must be diligent in implementing those practices every single day.

(Emphasis added.)

Security starts with a risk assessment to identify anticipated threats to the information assets, including an inventory of information assets to determine what needs to be protected. The next step is development and implementation of a comprehensive information security program to employ reasonable physical, administrative, and technical safeguards to protect against identified risks. This is the most difficult part of the process. It must address people, policies and procedures, and technology. It needs to include policies, assignment of responsibility, training, ongoing security awareness, monitoring for compliance, and periodic review and updating.

At the ABA Annual Meeting in August, 2014, the ABA adopted a resolution on cybersecurity that is consistent with this general approach:

> RESOLVED, That the American Bar Association encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations

---


46 Available at www.americanbar.org/content/dam/aba/images/abanews/2014am_hodres/109.pdf.
and is tailored to the nature and scope of the organization and the data and systems to be protected.

It recommends an appropriate cybersecurity program for all private and public sector organizations, which includes law firms.

The requirement for lawyers is reasonable security, not absolute security. New Jersey Ethics Opinion 701 states “[r]easonable care,” however, does not mean that the lawyer absolutely and strictly guarantees that the information will be utterly invulnerable against all unauthorized access. Such a guarantee is impossible…” Recognizing this concept, the Ethics 20/20 amendments to the Comment to Rule 1.6 include “…[t]he unauthorized access to, or the inadvertent or unauthorized disclosure of, confidential information does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.”

Security involves thorough analysis and often requires balancing and trade-offs to determine what risks and safeguards are reasonable under the circumstances. Considerations include the sensitivity of the information, the risks, and available safeguards (including their cost, difficulty of implementation, and effect on usability of the technology). There is frequently a trade-off between security and usability. Strong security often makes technology very difficult to use, while easy to use technology is frequently insecure. The challenge is striking the correct balance among all of these often competing factors. This aspect of security is also recognized by the Ethics 20/20 amendments.

**Reasonable Safeguards**

The greatest challenge for lawyers in establishing cybersecurity programs is deciding what security measures are necessary and then implementing them. Determining what constitute “competent and reasonable measures” can be difficult. The Ethics 20/20 amendments, discussed above, provide some high level guidance. As discussed above, the following factors are applied for determining reasonable and competent safeguards:

Factors to be considered in determining the reasonableness of the lawyer’s efforts 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).

A number of organizations have published security standards that can be used in determining reasonable security for a law firm. Examples include The SANS Institute’s *Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines*, currently in Version 4.0, the National Institute of Standards and Technology’s (NIST) standards in many areas, including “Small Business Information Security: the Fundamentals,” NISTIR-7621 (October 2009), and the International Organization for Standardization (ISO), 27000 series security standards.

---

47 Available at www.sans.org/critical-security-controls.


49 www.iso.org/iso/home.html.

ILTA (the International Legal Technology Association) has established the LegalSEC initiative, which is analyzing and adapting current standards and delivering a set of security policy and procedures templates tailored to law firms.53

As a final example of guidance, the ABA President appointed the ABA Cybersecurity Legal Task Force in 2012.54 Its focus includes security for law firms and clients, critical infrastructure security, and international cybersecurity issues. It has been working on security and data breach guidance for attorneys.

Protection of laptops, smartphones, tablets, and other mobile devices presents a good example of application of the requirement of “reasonable efforts” to a specific category of technology. Mobile devices present a great security risk because they can be easily lost or stolen. The Verizon 2014 Data Breach Investigation Report (covering 2013) explains the risk and a solution to it – encryption – this way:55

**PHYSICAL THEFT AND LOSS**  
**RECOMMENDED CONTROLS**

*The primary root cause of incidents in this pattern is carelessness of one degree or another. Accidents happen. People lose stuff. People steal stuff. And that’s never going to change. But there are a few things you can do to mitigate that risk.*

*Encrypt devices*

*Considering the high frequency of lost assets, encryption is as close to a no-brainer solution as it gets for this incident pattern. Sure, the asset is still missing, but at least it will save a lot of worry, embarrassment, and potential lawsuits by simply being able to say the information within it was protected.*

50  www.cert.org.
51  www.us-cert.gov.
52  www.cisecurity.org.
53  www.iltanet.org, click on “Publications,” then “LegalSEC.”
54  www.americanbar.org/groups/leadership/office_of_the_president/cybersecurity.html.
While each attorney and law firm have to determine what is reasonable in their circumstances, this raises the question, does failure to use encryption for mobile devices - a no-brainer solution – comply with the duty to employ reasonable safeguards?

Significantly, the Verizon 2013 Data Breach Investigation Report (covering 2012) reports that 78% of breaches were of low or very low difficulty for initial compromise. This suggests that basic and intermediate safeguards may have prevented many of them.

**Conclusion**

Attorneys have ethical and common law obligations to take competent and reasonable measures to safeguard information relating to clients. They also often have contractual and regulatory requirements. Compliance with these duties requires developing and implementing a comprehensive information security program. Important considerations for attorneys include understanding limitations in their competence, obtaining appropriate qualified assistance, continuing security training, and ongoing review and updating as technology, threats, and available security evolve over time. Particularly important is constant security awareness by all users of technology – every day, every time they’re using technology.

**Additional Information**

American Bar Association, Legal Technology Resource Center  
www.americanbar.org/groups/departments_offices/legal_technology_resources.html

American Bar Association, A Playbook for Cyber Events (American Bar Association 2013)

American Bar Association, Section of Science and Technology Law, Information Security Committee  
http://apps.americanbar.org/dch/committee.cfm?com=ST230002

ILTA (International Legal Technology Association), LegalSEC  
www.iltanet.org, click on “Publications,” then “LegalSEC.”

National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (February 2014)  


---

Ethical Implications of NSA Surveillance for Lawyers
by Sharon D. Nelson, Esq. and John W. Simek
© 2014 Sensei Enterprises, Inc.

It Seems Like Old News
At least once a week we are reminded that the cybersecurity of law firms is at risk from a newly
discovered source – The National Security Agency. After 9/11, many Americans embraced the Patriot
Act, numb from the tragedy and justifiably concerned about terrorist plots on American soil. After a
time, most folks became complacent and more or less bought the government’s reassurance that
federal surveillance involved primarily foreigners and that it was not snooping on the activities of
ordinary Americans.

That proved wrong in a big way. Courtesy of Edward Snowden (like him or hate him, he exposed a lot of
illegal and unconstitutional activities), we have learned that we are closer to the “Big Brother” state of
George Orwell’s “1984” than we ever thought possible. So let’s take a brief look at what we now know
and then we’ll turn to the implications for lawyers.

The NSA’s Bag of Tricks – and its Targets
Thanks again to Edward Snowden, The Washington Post published a story based on an internal National
Security Agency (NSA) audit and other top secret documents. The story indicates that the NSA has
broken privacy rules or overstepped its legal authority thousands of times each year since it was granted
broad new powers in 2008.

Most of the violations involved unauthorized surveillance of Americans or foreign intelligence agents in
the U.S., surveillance that is restricted under statute and Executive Order. They resulted in the
interception of U.S. e-mails and telephone calls.

How do they do that? Recent reports have indicated that the NSA is even intercepting shipments of
computers purchased online in order to infect them with spyware or replace components with its own
malware-installed hardware. That’s pretty gutsy. Of course you need to be specifically targeted by the
NSA before you’ll get a little “something extra” arriving along with the shiny new computer.

Suppose you didn’t order a new computer. How could the NSA intercept your data? Additional
revelations were disclosed at the Chaos Communications Congress. Apparently, there is a whole catalog
of equipment and software that the NSA is willing to sell to other agencies. One such device is called the
NIGHTSTAND. It is designed to hack WiFi devices from eight miles away. It is a standalone tool and can
exploit targets including Win2K, WinXP, WinXP SP1 and Win XP SP2 systems running Internet Explorer
version 5.0-6.0. There is no report that they have hardware for the more modern operating systems or
browsers. Yet another reason to make sure you are up to date with patches and versions.

What is XKeyscore?
Again by way of a Snowden leak, The Guardian revealed new details on a very powerful, secret program
run by the U.S. government called XKeyscore. With the program, NSA employees can obtain everything
from phone numbers to e-mail addresses. The NSA can also see e-mail content, Internet activity, browser history, and an IP address. According to the files and to Snowden, no warrant is needed.

**Microsoft Helps the NSA View Its Encrypted Data**
According to yet another article from *The Guardian*, citing top secret documents from you-know-who, Microsoft has:

- Helped the NSA circumvent its encryption so that the agency can intercept web chats on the Outlook.com portal
- Given pre-encryption stage access to e-mail on Outlook.com, including Hotmail
- Allowed the NSA easier access to SkyDrive
- Helped to triple the amount of Skype video calls being collected through Prism

**Mystic and Retro Tool**
In another report, the NSA has the ability to capture 100% of a foreign country’s telephone calls and then rewind and review them up to 30 days after they occurred. The released documents state that there is money budgeted to target five countries, but the countries are not identified. So much for protecting the client/attorney privilege, especially if your client is in a targeted country.

**A Little Help from Our Friends**
As if the global surveillance capabilities of the NSA aren’t enough, we have our friends from the Five Eyes Alliance (United States, United Kingdom, Canada, Australia and New Zealand) helping out too. The *New York Times* reported that the NSA’s Australian counterpart, the Australian Signals Directorate, notified the agency that they were conducting surveillance of trade talks between Indonesian officials and an American law firm. Of course they were willing to share the information. The law firm is yet to be identified (though thought to be Mayer Brown), but capturing privileged communications doesn’t appear to be limited to the NSA.

**Soooo - How is a Law Firm to Keep its Data Confidential?**
The NSA revelations have serious implications for lawyers. We used to tell lawyers that Skype was secure – but then Microsoft bought it and began changing the network architecture by running the calls through its servers – and now, apparently, unlocking data for the NSA from time to time. And what about the lawyers who are storing their data in SkyDrive? Or the solos who are using Hotmail?

**Battening Down the Hatches**

**Cloud Computing**
Roughly half of all law firms are now holding at least some data in the cloud. The recent news has shaken them, as well it should. But we are not preaching a mass exodus from the cloud. Two major points here:
• If you are fundamentally storing all your data in a datacenter, your biggest problem is whether the datacenter personnel can gain access to your data. For this reason, we do not recommend putting law firm data on servers owned by the datacenter. It doesn’t matter whether there is a master decryption key or whether a “back door” is built in. The safest way to store data in a datacenter is to use a hybrid solution – where you own the equipment and the access to your equipment and data is restricted to yourself and your own IT folks in locked racks. Any emergency access to the data, by contract, should require immediate reporting to you and, again by contract, you should receive notice of any law enforcement request for the data right away so you can file a motion to quash. Major players in the market may not give you these terms but the smaller ones will. One caveat: If a request is made under The Patriot Act, you’re toast – your data will be handed over on a silver platter. But the vast majority of law enforcement requests are not made pursuant to the Patriot Act.

• If you are using specific clouds to store data, encrypt your data before sending it. A great example is Dropbox, now utilized by so many litigators. If you encrypt your Word or PDF documents before putting them in Dropbox, it doesn’t matter that Dropbox holds a master decryption key (and it does). Even if it attempts to decrypt for the federal agents at the door, Dropbox can only provide them with garbage. What the feds can do with the data is apparently changing. News reports indicate increasing success in breaking encryption, but we have yet to see proof. And yes, encryption will work for SkyDrive, the iCloud (depending on the data type and device used), etc. And no, this is not hard. Stop being afraid of the word encryption. If you password protect a Word or PDF document (which you can do natively within the program – just search “Help”), it is encrypted. Just promise us you won’t send it as an attachment with the decrypt key in the text of the e-mail.

Encryption
You should also be taking a hard look at encryption on your smartphones – iPhones are encrypted when configured with their PINs, poorly with a 4 digit pin – you need a complex password. BlackBerrys are natively encrypted when “Content Protection” is enabled. Android encryption must be turned on in Settings, but it is there.

No lawyer should be performing work on a personal machine. In today’s world, every lawyer should be issued a firm laptop and smartphone so that security can be controlled and monitored. This means no BYOD unless you are prepared to implement a MDM (Mobile Device Manager) solution to the tune of several thousands of dollars. All laptops, like smartphones, should have whole disk encryption.

Bottom line...you should be encrypting data on all devices. The one disclaimer is the recent news concerning the capabilities of the NSA. As noted security commentator, Bruce Schneier, has stated, “The NSA is breaking most encryption on the Internet.” This is accomplished by intercepting the data and compromising the secure certificate provider infrastructure or using intentional weaknesses inserted in encryption products. As an example, RSA Security released an advisory to stop using the Dual Elliptic Curve Deterministic Random Bit Generation (Dual EC DRBG) because of weaknesses in the algorithm.
Apparently, the NSA had their fingers in the design of Dual EC DRBG. Some have even suggested using encryption and security products from vendors that are not based in the United States to minimize any potential NSA back doors. The good news is that a large number of products do not use the flawed Dual EC DRBG. Remember, we are only talking here about compromising SSL certificates – not all encryption.

And, happily, Mr. Schneier has also noted that “strong encryption makes the NSA batty.” So strong encryption sounds like a good prescription for law firms.

Secure Communications
Now that we know the NSA (and others) have the ability to capture huge quantities of communications (voice, text, e-mail, etc.), you should consider whether some method of secure communication should be used. Encryption is your friend. There are several methods and services available to encrypt e-mail or the attachment contents as previously mentioned. Encrypted voice and text communication is also possible. Mobile apps such as RedPhone or TextSecure allow for encrypted voice and text communications. Another alternative is to purchase the Blackphone, which provides encrypted voice and text communication built into the handset itself.

Security audits
We used to say that you needed security audits every 6-12 months to keep the Chinese and the cybercriminals out of your networks. Now we add that you need to protect your networks against our own government – sad but true. By in large, big firms will go to big companies to perform these audits. Solos and small will head to smaller firms where the price tag isn’t so high. Get a referral from trusted friends, check out credentials, etc. – but don’t fail to do these audits.

Parting Words
With all the examples of the NSA “data capture” projects, we have changed our advice to lawyers concerning protection of client data. We believe it is now a lawyer’s ethical duty to address confidentiality in any engagement letter and get informed consent from the client as to what measures need to be taken to protect the potential collection of client communication. Lest we seem overly paranoid, we’ll give the parting words to George Washington – who better than the father of our country?

“Government is not reason; it is not eloquent; it is force. Like fire, it is a dangerous servant and a fearful master.”

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone)
www.senseient.com
RESOLUTION APPROVED BY THE ABA HOUSE OF DELEGATES 8/12/14

"RESOLVED, That the American Bar Association encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected."

The Resolution was far shorter than the original version and the accompanying Report makes it clear that there is no intent to impose any new ethical obligations on lawyers and emphasizes that the suggested course of action may have different parameters for small businesses and law firms.

After many compromises along the way caused by the input of other entities, there was no opposition to the Resolution.

REPORT

(Note that this Report had not been finalized and placed online by the time of submission of these materials -- the authors have been told that substantial changes are not anticipated)

I. INTRODUCTION

This Resolution addresses cybersecurity issues that are critical to the national and economic security of the United States (U.S.). It encourages private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected. This Resolution and Report are intended to educate organizations and heighten their sensitivity to cybersecurity risks, and help them effectively evaluate their own specific risks and respond on behalf of their organization. The Resolution and Report do not define any obligations pursuant to laws or rules, including applicable lawyers’ rules of professional conduct.

Recognizing that small businesses, small law firms and solo practitioners have varying financial and human resources available to them, the components of a cybersecurity program should be flexible and their implementation should be practical.

II. CYBERSECURITY THREATS -- BACKGROUND

The threat environment today is highly sophisticated, and massive data breaches are occurring with alarming frequency. Cyber-criminals exploit weaknesses in software and operating platforms, the domain name system, and mobile and web-based applications. They conduct successful social engineering through phishing attacks, social media, email, and various applications. Malware can quickly morph, change security controls, lurk in systems undetected, download other malware, and exfiltrate data undetected.
An organization-wide cybersecurity program with defined controls based on risk categorizations reflecting the operational impact and magnitude of harm of a cyber incident can mitigate risk to a considerable degree. In many cases, data breaches or other types of cyber incidents could have been prevented or detected early and the risks of the incident mitigated if the organization had undertaken proper security planning and implemented appropriate security safeguards.

In today’s digital world, threats to data and information systems are found almost everywhere a computer, server, smart phone, thumb drive, or other electronic device is operating (including the cloud). Many organizations provide access to their networks to business partners and entrust their data and business functions to outsourcing and cloud providers, creating additional risks. The proliferation of mobile devices and wireless technologies that enable mobile commerce and a continually expanding array of applications—more than 1.5 million—also present vulnerable points in the flow of sensitive data in computer networks.

Security is only as strong as its weakest link. Failed security has resulted in thousands of data breaches that have led to the loss or compromise of millions of personally identifiable records, as well as the theft of classified information, valuable intellectual property and trade secrets, and the compromise of critical infrastructure.57 The consequences of a cyber incident or data breach can have a disturbing impact on the victim, whether a business, organization, government entity, or an individual.

The protection of one of the most valuable and vulnerable assets of all organizations—its information—is not only vitally important, but it also avoids the high costs associated with cybercrime, including forensic investigations and data breach notification; the loss of confidential, classified, and proprietary data; reputational damage; loss of public confidence; and in the case of business, drops in stock price, and loss of market share and trust. Breaches also have resulted in the disclosure of closely-held government information, and businesses have faced regulatory fines and investigations, civil damage actions, administrative proceedings, and criminal indictments. The first- and third-party losses associated with security incidents are rising, and cybersecurity is now one of the top risks organizations must manage.

Sensitive Data At Risk

There are many types of sensitive data that are targeted by cyber-criminals or subject to unauthorized access, use, disclosure, or sabotage by insiders. They include personally identifiable information (PII), personal health information (PHI), and financial records, confidential and proprietary business data, intellectual property and trade secrets, research data, privileged legal documents, and classified information (including sensitive national security information). There is a vibrant market for these data, and all organizations—regardless of size—should consider themselves at risk.

The sensitive personal data being amassed by companies and governments is staggering. Inexpensive storage has enabled companies to collect and store large amounts of data and retain it far longer than they would have if it were in paper. “Big data,” the term applied to the

collection of massive amounts of data that can be correlated, analyzed, and parsed for targeted advertising and strategic business purposes, creates rich targets for cyber-criminals. PII that can be used for fraud is being collected and often stored by organizations unprotected, putting many Americans at risk.58 On its website, the Internal Revenue Service (IRS) indicates that it “has seen a significant increase in refund fraud that involves identity thieves who file false claims for refunds by stealing and using someone's Social Security number.”59

Another aspect of the problem is illustrated by the dependence of American society on electronic transactions and e-commerce, which has fueled data breaches in all industry sectors. Failed security has resulted in massive data breaches of millions of personally identifiable records.60 The recent data breaches of leading retail companies and credit bureaus have caught the attention of the public, politicians, and law enforcement. The success of these breaches, however, has also created a “me too” among cyber-criminals eager to capture their own trove of data. Risks will increase with the “Internet of Things,” as the Internet becomes the backbone for appliances, gadgets, and operational aspects of daily life. Many of the most personal aspects of people’s lives will be documented and transmitted over the Internet, subject to interception or theft.

Protecting the Nation’s Critical Infrastructure

The national and economic security of the United States depends on the reliable functioning of critical infrastructure: cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation’s security, economy, and public safety and health at risk. Similar to financial and reputational risk, cybersecurity risk affects a company’s bottom line. It can drive up costs and impact revenue. It can harm an organization’s ability to innovate and to gain and maintain customers.61


Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience, issued in February 2013, advances a national policy to strengthen and maintain secure,

functioning, and resilient critical infrastructure. Comprehensive cybersecurity programs are essential for critical infrastructure organizations, and following appropriate security frameworks and standards is central to achieving a strong cybersecurity posture and resilience. The electric sector, for example, voluntarily agreed to comply with cybersecurity requirements promulgated by the North American Electric Reliability Corporation and the Federal Energy Regulatory Commission (NERC/FERC).

The National Institute of Standards and Technology (NIST) recently published the Framework for Improving Critical Infrastructure Cybersecurity, and mapped the Framework to other accepted security frameworks and standards.

### Law Firms Are Targets of Cyber Attacks

The threat of cyber attacks against law firms is growing. Lawyers and law firms are facing unprecedented challenges from the widespread use of electronic records and mobile devices. There are many reasons for hackers to target the information being held by law firms. They collect and store large amounts of critical, highly valuable corporate records, including intellectual property, strategic business data, and litigation-related theories and records collected through e-discovery.

The data and information kept by law firms are largely protected by the attorney-client privilege and/or the work product doctrine, as well as by various legal ethics requirements. Thus, lawyers and law firms should implement an appropriate cybersecurity program to protect confidential and sensitive information.

Both large and small law firms have been the target of hacker attacks in the U.S. as well as abroad. The FBI has issued warnings to firms and held a meeting in early 2012 with approximately 200 law firms in New York City to discuss the risk of breaches and theft of client data. A cybersecurity firm that helps organizations secure their networks against threats and resolve computer security incidents estimated that 80 major law firms were breached in 2011 alone.

The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals (2013) provides threat information, practical guidance and strategies to lawyers and law firms of all sizes, and explores the relationship and legal obligations between lawyers and clients when a cyber-attack occurs. Amendments to the ABA Model Rules of Professional Conduct (Model Rules) adopted in 2012 provide that a lawyer’s duty of competence includes keeping abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology (Comment [8] to Model Rule 1.1). Further, to enhance the protection of client confidential information, Model Rule 1.6 (Confidentiality) provides 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.” The touchstone regarding lawyers’ obligations under Model Rules 1.1 and 1.6 is reasonableness. What is reasonable depends on the circumstances. With regard to data security, the Comments to Model Rule 1.6 provide lawyers with a nonexclusive list of factors designed to help them assess the reasonableness of their actions.

III. CYBERSECURITY PROGRAM—FRAMEWORKS AND STANDARDS

There are a number of accepted frameworks and standards that can serve as a reference for developing, implementing, and maintaining an appropriately-tailored cybersecurity program. Some of these well-known frameworks and standards include:

- Information Technology Infrastructure Library (ITIL), http://itil-officialsite.com
- International Society of Automation (ISA), http://www.isa.org
- ISACA, COBIT, http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx
- U.S. Nuclear Regulatory Commission, nrc-stp.ornl.gov/slo/regguide571.pdf

These references are generally consistent, and a number of the provisions in the various security frameworks and standards map to one another. Thus, it is less important which framework or standard an organization might choose to follow and more important that it undertakes the key activities of a cybersecurity program.

A cybersecurity program is comprised of a series of activities. These activities include, for

example: governance by boards of directors and/or senior management; development of security strategies, plans, policies and procedures; creation of inventories of digital assets; selection of security controls; determination of technical configuration settings; performance of annual audits; and delivery of training.

Due to the nature of the threat environment, certain activities in a cybersecurity program are ongoing. Continuous monitoring and log analysis are designed to provide data that can provide early detection of threats. To maintain a proactive security posture, potential threats should be investigated and targeted attacks detected in advance or addressed as they occur. The objective is to address cybersecurity threats and risks in a timely, disciplined, and structured fashion.

Privacy compliance requirements should be incorporated into the cybersecurity program. In addition, an effective cybersecurity program requires trained personnel to evaluate the security impact of actual and proposed changes to the system, assess security controls, correlate and analyze security-related information, and provide actionable communication of the security status across all levels of the organization.

Administrative, technical, organizational and physical controls help ensure the confidentiality, availability, and integrity of digital assets. Such controls should be carefully determined, implemented, and enforced. NIST has published extensive guidance on the selection of controls for government systems, which can also be useful for private sector organizations.66

Many organizations are undertaking some of the required cybersecurity activities, but not others, and some activities may be performed without all the critical inputs. In such cases, the resulting cybersecurity program could have gaps and deficiencies and associated risks that may adversely affect the organization’s operations, financial bottom line, and compliance. To help protect against massive data breaches or loss of confidential/proprietary data, organizations—whether private or public—should continually work to assess and improve their security posture, in light of the most recent guidance and recommendations on cybersecurity programs.

Small Organizations

Recognizing that small businesses, small law firms and solo practitioners have varying financial and human resources available to them, the components of a cybersecurity program should be flexible and their implementation should be practical. Small organizations, including small law firms and solo practitioners, can prioritize key cybersecurity activities and tailor them to address the specific risks that have been identified. For example, NIST has provided guidance on information security for small businesses67 Similarly, the U.S. Department of Health and Human Services (HHS) has accorded flexibility in its HIPAA Security Series guidance for the needs of

small covered entities. 68

IV. RISK-BASED ASSESSMENT—AN ACCEPTED BUSINESS PROCESS

Organizational risk can include many types of risk (e.g., management, investment, financial, legal liability, safety, logistics, supply chain, and security risk). Security risks related to the operation and use of information systems is just one of many types of organizational risk. This Resolution focuses on one aspect of a comprehensive enterprise risk management program—operational and IT/cyber risk.

Risk assessments inform decision-makers and support the risk management process by identifying: (i) relevant threats to the organization or threats directed through third party entities; (ii) vulnerabilities both internal and external to the organization; (iii) the impact (i.e., harm) to the organization and individuals that may occur given the potential for threats exploiting vulnerabilities; and (iv) likelihood that harm will occur. The end result is a categorization of risk according to the degree of risk and magnitude of harm to the organization flowing from the threat or vulnerability if it occurred.

Cybersecurity is based on a systematic assessment of risks that are present in a particular operating environment. Ensuring the confidentiality, integrity, and availability of digital assets is fundamental to their protection. Risk assessments are undertaken to identify gaps and deficiencies in a cybersecurity program due to operational changes, new compliance requirements, an altered threat environment, or changes in the system architecture and technologies deployed.

Risk assessments are the basis for the selection of appropriate security controls and the development of remediation plans so that risks and vulnerabilities are reduced to a reasonable and appropriate level. The principal goal of the organization’s risk management process should be to protect the organization and its ability to perform its mission, not just to protect its IT assets.

Risk assessment is not new to most businesses. It is a fundamental business process that many have been following since at least 1977 when Congress enacted the requirement in the Foreign Corrupt Practices Act of 1977 (FCPA), 15 U.S.C. §§ 78dd-1, et seq., that public companies have internal controls. Nearly all rely on the COSO Framework to comply with the internal control reporting requirements under the FCPA and the Sarbanes-Oxley Act of 2002, PL 107-204, 116 Stat 745. 69. The framework, issued in 1992 and updated in 2013, is designed to assist companies in structuring and evaluating controls that address a broad range of risks. It is geared to the achievement of three important objectives—operations (operational and financial reporting goals, and safeguarding assets from loss, the objective of an effective cybersecurity program), reporting (financial and non-financial), and compliance (with laws and regulations).


69 The Committee on Sponsoring Organizations of the Treadway Commission (“COSO”), an initiative of several groups with an interest in effective internal control, available at http://www.coso.org.
Risk assessments for publicly-traded companies are addressed in the Securities and Exchange Commission (SEC) guidance on *Disclosure by Public Companies Regarding Cybersecurity Risks and Cyber Incidents*.

Examples of cybersecurity risk management frameworks and standards include:

- **ISO/IEC 27005:2011: *Information Security Risk Management*.** It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the implementation of information security based on a risk management approach.

- **ISO/IEC 31000:2009: *Risk Management—Principles and Guidelines*.** This document is intended to harmonize risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks and/or sectors, and does not replace those standards. It can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.


- **Critical Sectors—DHS Infrastructure Risk Management Approach.** This guidance provides a useful approach to critical infrastructure risk management utilizing a risk management framework enunciated by DHS. It is designed to be applied to all threats and hazards, including cyber incidents, natural disasters, man-made safety hazards, and acts of terrorism, although different information and methodologies may be used to understand each. Risk information allows partners, from facility owners and operators to federal agencies, to prioritize their risk management efforts.

---


• *DOE Electricity Subsector Cybersecurity Risk Management Process (RPM).* The electricity subsector increasingly relies on digital technology to reduce costs, increase efficiency, and maintain reliability during the generation, transmission, and distribution of electric power. Managing cybersecurity risk is critical to achieving their strategic goals and objectives, including reliability, resiliency, security, and safety. Issued by the Department of Energy in conjunction with NIST and NERC, this guidance is designed to help utilities better understand their cybersecurity risks, assess severity, and allocate resources more efficiently to manage those risks.

V. **CYBERSECURITY PROGRAM—CYBER RESPONSE PLANS**

Incident response is the practice of detecting a problem, determining its cause, minimizing the damage it causes, resolving the problem, and documenting each step of the response for future reference. Fully developed and tested incident response plans and business continuity/disaster recovery (BC/DR) plans are components of a cybersecurity program. Organizations should be prepared if a cyber attack or data breach occurs or if an event interrupts their operations. Response plans, policies, and procedures should be able to accommodate the full array of threats, not just data breaches.

Incident response plans involve stakeholders across an organization, including IT, security, legal, finance, operational units, human resources, and procurement. The individuals should be identified and their roles and responsibilities defined. Communication with and coordination among stakeholders is an important aspect of an incident response plan. This includes the identification of who within an organization should be responsible for communicating with employees, customers, and other key groups (e.g., investors). It would also include plans for appropriate external communications, such as with first responders, forensic investigation experts, Computer Emergency Response Teams (CERTs), Information Sharing and Analysis Centers (ISACs), regulators, communications providers, and outside counsel.

If litigation is anticipated, adequate documentation and evidentiary procedures for incident response can be very important. This advance planning can help to ensure that valuable tracking and tracing data and evidence of what happened within a system are preserved and secured and chain of custody is documented.

For many organizations, adequate incident response planning is a compliance requirement. For example, those organizations subject to the Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), or state data breach laws.

Resources are available to assist organizations in understanding the key components of incident response. NIST, for example, has published an excellent guide, the *Computer Security Incident*

---


Business Continuity Management—The other critical cyber response plan for a cybersecurity program is a business continuity/disaster recovery plan. Although they are commonly lumped together as BC/DR, there are separate processes for business continuity and disaster recovery. A cybersecurity incident that is initially handled under an incident response plan may cause a business interruption that requires implementation of business continuity procedures. Thus, each plan should be drafted and tested for such circumstances to ensure a smooth and efficient response and continuity of operations.

Certain critical infrastructure sectors have BC/DR requirements. NERC, for example, has requirements for BC/DR in its required standards, and it conducts ongoing work regarding continuity of operations and resiliency of electricity grids. These activities help these companies stay abreast of threats and develop, implement, and maintain sophisticated BC/DR plans.

VI. INFORMATION SHARING

Sharing threat information regarding cyber incidents with others, such as law enforcement, community emergency response teams (CERTs), information sharing and analysis centers (ISACs), business partners, and public sector cyber officials who could benefit from the knowledge, helps advance cyber defenses and resiliency in other organizations. An attack on any organization may impact others, or it may be targeted at a particular activity or business process, such as point-of-sale systems or control processes. The sharing of threat information can substantially improve the ability of other organizations to respond to a similar attack. It also expands the knowledge base about threats and effective mitigation measures.

Many organizations have not thought through what external assistance they might need when responding to incidents. Establishing relationships with external organizations—such as FBI InfraGard, ISACs, CERTs, and industry cyber groups—regarding cyber threats can be an important defensive measure for any organization. Such organizations are usually open to receiving information in an anonymized or sanitized fashion, if desired, by the entity providing the information.

80 Lawyers, law firms, and organizations and entities authorized to provide legal services should take into consideration any ethical constraints that may apply to client records, and any legal restrictions applicable to records under seal, grand jury information, classified information, etc.
It is important that organizations identify what data they might share, determine with whom they would share it and in what form, and consider any legal ramifications associated with the data or sharing it with third parties. Although some have raised concerns that antitrust constraints may arise with information sharing, the U.S. Department of Justice (DOJ) has indicated a willingness to provide letters of exception, if requested, to enable cyber information sharing. On April 14, 2014, DOJ joined with the Federal Trade Commission (FTC) and issued a joint “Antitrust Policy Statement on Sharing of Cybersecurity Information,” which clarifies the issue:

Through this Statement, the Department of Justice’s Antitrust Division (the “Division”) and the Federal Trade Commission (the “Commission” or “FTC”) (collectively, the “Agencies”) explain their analytical framework for information sharing and make it clear that they do not believe that antitrust is—or should be—a roadblock to legitimate cybersecurity information sharing.81

VII. EXISTING ABA POLICY

In recent years, the ABA House of Delegates and Board of Governors have adopted several policies regarding cybersecurity and lawyers’ use of technology, and the proposed Resolution is consistent with those existing ABA policies. These ABA policies include the following:

Resolution 118, Adopted by the House of Delegates at the 2013 Annual Meeting in San Francisco (August 2013)

This Resolution condemns intrusions into computer systems and networks utilized by lawyers and law firms, urges federal, state, and other governmental bodies to examine and amend existing laws to fight such intrusions, and makes other related recommendations. The complete Resolution and Report are available at:

http://www.americanbar.org/content/dam/aba/administrative/law_national_security/resolution_118.authcheckdam.pdf

* * *

Policy Adopted by the ABA Board of Governors (November 2012)

The ABA's Board of Governors approved a policy in November 2012 comprised of five cybersecurity principles developed by the ABA Cybersecurity Legal Task Force. The complete Resolution and Report are available at:

http://www.americanbar.org/content/dam/aba/marketing/Cybersecurity/aba_cybersecurity_res_and_report.authcheckdam.pdf

* * *


Resolution 105A amends the black letter and Comments to Model Rule 1.0 (Terminology), the Comments to Model Rule 1.1 (Competence) and Model Rule 1.4 (Communication), and the black letter and Comments to Model Rule 1.6 (Confidentiality of Information) and Model Rule 4.4 (Respect for Rights of Third Parties) of the ABA Model Rules of Professional Conduct dated August 2012, to provide guidance regarding lawyers’ use of technology and confidentiality. Resolution 105B amends the black letter and Comments to Model Rules 1.18 and 7.3, and the Comments to Model Rules 7.1, 7.2 and 5.5 of the ABA Model Rules of Professional Conduct dated August 2012, to provide guidance regarding lawyers’ use of technology and client development.

Resolution 105C amends the Comments to Model Rule 1.1 (Competence) and Model Rule 5.5 (Unauthorized Practice of Law; Multijurisdictional Practice of Law), and the title and Comments to Model Rule 5.3 (Responsibilities Regarding Nonlawyer Assistants) of the ABA Model Rules of Professional Conduct dated August 2012, to provide guidance regarding the ethical implications of retaining lawyers and nonlawyers outside the firm to work on client matters (i.e., outsourcing).

The Resolutions and the related Reports are available at:

http://www.americanbar.org/content/dam/aba/directories/policy/2012_hod_annual_meeting_105a.doc

http://www.americanbar.org/content/dam/aba/administrative/law_national_security/resolution_105b.authcheckdam.pdf

http://www.americanbar.org/content/dam/aba/directories/policy/2012_hod_annual_meeting_105c.doc

VIII. CONCLUSION

This Resolution is intended to call attention to the importance of appropriate cybersecurity programs for all organizations. These issues are linked directly to our Nation’s economic and national security. The principles and concepts discussed in this Resolution and Report can help organizations, including law firms, understand and address cybersecurity threats and risks.

Respectfully Submitted,

Judith Miller
Harvey Rishikof
Co-Chairs, ABA Cybersecurity Legal Task Force

August 2014
Too often, law firm managing partners are content to let their IT departments operate on cruise control – until a crisis strikes. There are so many questions that they should be asking that it was hard to winnow our list down to 10.

1. How do we ensure that we are installing all critical updates and patches for our software and hardware? Believe it or not, this is the number reason for data breaches – the failure to patch. There should be a reporting mechanism so that you receive weekly reports of all updates made – you don’t have to read it, but at least there will be an audit trail – and making the report will constantly remind your IT director to be vigilant.

2. How often do we require passwords to be changed and what are our rules for password strength? Today, sadly, the answer should be every 30 days (no repeats) 12 characters, using upper and lower case, numbers, and special characters.

3. How are we preparing to move beyond passwords? Passwords will be obsolete in the near future. Google is already moving to two factor authentication and has announced that it will move away from “passwords only” in the future. Biometrics is one option, but we prefer two factor authentication using some kind of token (something you physically have) in addition to a password (which now doesn’t have to be as complicated).

4. What is our process for securing data when we terminate employees? There should be a checklist of items to go through, including the return of all data, killing IDs and the ability to connect remotely, retrieving all firm cell phones, laptops, prox cards, keys, etc. If they have a personal code to get in the office, terminate the code. The list is long.

5. Do we change the defaults on all our equipment? This is the second most common reason for breaches – default are unchanged on routers, etc. and
even the script kiddies (never mind the true cybercriminals) know all the defaults. There should be reports verifying this as well.

6. What is our incident response plan? If you suffer a breach, is there a team in place? Who needs to be notified? Do you have a digital forensics company that you can call to investigate and remediate a breach? Do you have an attorney who is a data breach specialist who can assist in helping you comply with any federal or state notification laws and regulations? Another long list here.

7. Do we have redundant hot and cold backups and a plan for business continuity in the event of an emergency?

8. Do we have a Bring Your Own Device (BYOD) policy? If so, have we recently evaluated the risks of having personal devices connected to our network?

9. Are we storing data in the cloud? If so, make sure that a lawyer has actually read the Terms of Service and your IT Director has adequately investigated the cloud for physical and data security – including whether the provider will advise you of any law enforcement requests for your data in time for you to file a Motion to Quash. No notice will be given if the requests are under the Patriot Act, but most of them are not.

10. How are we protecting mobile data? Do all laptops have full disk encryption? Do we have adequate remote access policies? When attorneys connect remotely, is the data encrypted in transit?

There could be 100 questions – easily – but start with these 10 to get a handle on how well you are securing your law firm data!

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com.
Law Firm Data Breach Nightmares and How to Prevent Them

By Sharon D. Nelson, David G. Ries, and John W. Simek
© 2013 Sensei Enterprises, Inc.

Sharon D. Nelson is the president of Sensei Enterprises Inc., a digital forensics, information security, and information technology firm in Fairfax, Virginia. The author of 10 books and many articles, Nelson speaks frequently on legal technology, information security, and electronic evidence topics; writes the electronic evidence blog Ride the Lightning; and cohosts the ABA podcast series “The Digital Edge: Lawyers and Technology.” She is President of the Virginia State Bar and will become its president in June. She can be reached at snelson@senseient.com.

David G. Ries is a partner in the Pittsburgh, Pennsylvania, office of Thorp Reed & Armstrong, LLP, where he practices in the areas of environmental, commercial, and technology litigation. He frequently speaks and writes on legal ethics, technology, and technology law issues and is a contributing author to Information Security: A Legal, Business, and Technical Handbook, Second Edition (ABA 2011). He can be reached at dries@thorpreed.com. John W. Simek is the vice president of Sensei Enterprises Inc., noted above. A nationally recognized digital forensics technologist with multiple certifications, he has testified as an expert witness throughout the United States and provides information technology support to over 220 area law firms, legal entities, and corporations. Simek is a coauthor of nine books and hundreds of articles and speaks frequently on legal technology, information security, and electronic evidence. He can be reached at jsimek@senseient.com. This article is adapted and updated from the authors’ book Locked Down: Information Security for Lawyers (ABA 2012). To order, visit the ABA Bookstore online at www.ShopABA.org; see more information about the book on page 25.

Can Your Law Firm Be Breached?
In the paper world, it was remarkable when a law firm installed glass-breakage sensors on the windows of its 43rd floor conference room, where documents were compiled for big cases and deals. The firm wanted to ensure that no one could rappel from the skyscraper’s observation deck and break through the windows to steal the information. Boy oh boy, have times changed.

For years, we’ve been warning lawyers that it’s not a question of whether law firms will become victims of successful hacking attacks—it’s a matter of when. We pointed to numerous law firm incidents of dishonest insiders and lost or stolen laptops and portable media, but there were not disclosed incidents of successful hacking attacks.

We’ve now reached the “when”—successful attacks have occurred and are occurring—and attorneys and law firms need to address security. Law firm data in computers and information systems faces substantial and real threats. The American Bar Association’s (ABA’s) 2012 Legal Technology Survey Report states that 15.4 percent of law firms with 10 to 49 lawyers reported that their firm had experienced some kind of security breach in the past. In addition, 9.7 percent of all firms reported that they had suffered a security breach.

A November 2009 FBI alert warned that law firms and public relations firms were being targeted with spear phishing e-mails containing malicious payloads.¹ In January 2010, the FBI issued another alert, this time warning law firms about counterfeit check schemes that used e-mails to lure them into relationships with fraudulent overseas “clients.”²


In March 2010, the *San Francisco Chronicle* discussed recent attacks, ranging from phishing scams to intrusions into a law firm network to steal lawsuit-related information. It noted, “Security experts said criminals gain access into law firms’ networks using highly tailored schemes to trick attorneys into downloading customized malware into their computers. It is not uncommon for them to remain undetected for long periods of time and come and go as they please, they said.”

A March 2010 *National Law Journal* article reported that Mandiant, a leading information security firm that specializes in investigations of data breaches, had assisted over 50 law firms after security breaches. A Mandiant forensics specialist stated in an interview that Mandiant spent approximately 10 percent of its time in 2010 investigating data breaches at law firms.

Successful attacks on law firms have continued. In January 2012, *Bloomberg* described a group of major hacking incidents in which attackers successfully targeted seven Canadian law firms and two Canadian government agencies. The article reports that Mandiant estimated that 80 major law firms were hacked during 2011.

In November 2011, the FBI held a meeting for the 200 largest law firms in New York to advise them about the increasing number of attacks. *Bloomberg* reported the following about the meeting:

> Over snacks in a large meeting room, the FBI issued a warning to the lawyers: Hackers see attorneys as a back door to the valuable data of their corporate clients. “We told them they need a diagram of their network; they need to know how computer logs are kept,” Galligan [the head of the FBI cyber division in New York City] said of the meeting. “Some were really well prepared; others didn’t know what we were talking about.”

The SANS Institute, a highly regarded information security research, education, and certification organization, has published an interview with the managing partner and IT partner of a New York law firm that was hacked. They stated that all of their client files were found by the FBI on a server overseas.

A June 2012 *Wall Street Journal* article began:

> Think knowing how to draft a contract, file a motion on time and keep your mouth shut fulfills your lawyerly obligations of competence and confidentiality? Not these days. Cyberattacks against law firms are on the rise, and that means attorneys who want to protect their clients’ secrets are having to reboot their skills for the digital age.

The article discussed the ABA Commission on Ethics 20/20’s proposals on technology and confidentiality. They were adopted at the ABA Annual Meeting in August 2012, including amendments to Model Rules 1.1 and 1.6 that expressly require attorneys to take competent and reasonable measures to safeguard information relating to clients.

Most recently, the FBI gave a keynote presentation on law firm security threats at LegalTech New York in January 2013. The special agent in charge of the FBI’s cyber operations in New York City stated, “We have hundreds of law firms that we see increasingly being targeted by hackers . . . . We all understand that the cyberthreat is our next great challenge.
Cyber intrusions are all over the place, they’re dangerous, and they’re much more sophisticated” than they were just a few years ago.\(^\text{10}\)

Security threats to lawyers and law firms are substantial. It is critical for attorneys and law firms to address them through comprehensive information security programs. A data breach is likely to have numerous negative impacts for law firms, causing disruption, breakdowns in client relationships, publicity nightmares, great expense, and more. Now consider the fact that most lawyers do not have cyberinsurance that will cover the expense of complying with data breach laws, which now exist in 46 states, the District of Columbia, and the Virgin Islands. A single data breach could be a financial disaster for a small law firm.

The last stumbling block for lawyers who are disinclined to focus on security issues is their belief that it won’t happen to them—particularly their belief that no one would be interested in their data. Most of us can understand why merger and acquisition firms would be a magnet for hackers—clearly there is a great deal of money to be made on Wall Street with insider information. Fewer people think about the money to be made by having an insider’s knowledge of litigation, particularly in large suits involving a major corporation, where the result is likely to influence the stock market.

But what about small law firms? What attractive data do they hold? Many small firms practice family law—and their computers contain Social Security numbers, birth dates, credit card numbers, and other detailed financial information. This is precisely the kind of data that identity thieves are looking for. They routinely scan for vulnerable systems seeking such data.

Business espionage is another motivation for breaking into law firms. Perhaps you represent a company and a competitor wishes to acquire business intelligence from you. There also is the press. In 2011, the News of the World notoriously hacked into cell phones to feed the public’s insatiable appetite for gossip. Consider all the interest in a murder trial—is it conceivable that a reporter might seek private information to get a scoop? Of course. As we write this in February 2013, the New York Times and the Wall Street Journal have recently been hacked, as has Twitter and the Department of Energy. As the old saying goes, there is nowhere to run and nowhere to hide.

**Need More Convincing?**

Take a look at Privacy Rights Clearinghouse’s “Chronology of Data Breaches” from 2005 (when the first big breaches hit) to the present (www.privacyrights.org/data-breach). The first thing you’ll note is that there are lots of data breaches each month. The second thing you’ll note is that you don’t see a lot of law firms there. It is an open secret that law firms have played breaches very close to the vest and demand strict confidentiality agreements from information security vendors who investigate any compromise of their networks. This of course means there are law firms out there that have chosen not to comply with state data breach notification laws, which frankly doesn’t surprise us.

The third thing you’ll notice is that there are a ton of health industry breaches here. Why? Because there is a federal law requiring that this industry report breaches and the law has teeth. The Health Information Technology for Economic and Clinical Health (HITECH) Act, which was enacted as part of the American Recovery and Reinvestment Act of 2009, contains several significant changes to the privacy rules contained in the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The HITECH Act requires that covered entities subject to the HIPAA privacy rule and their business associates must provide notice when unsecured protected health information has been breached. In spite of the law and the number of breaches
you see reported, a study by the Healthcare Information and Management Systems Society (HIMSS) found that only 11 percent of medical practices are likely to report an incident of medical identity theft—in spite of all the state laws requiring a report.11

If a federal law is passed that covers personal information generally and provides stiff penalties, you’ll be seeing a lot more industries in the “Chronology of Data Breaches”—and you’ll probably find that law firms, always seeking to keep embarrassing information private, may well be like the medical practices and take their chances with flaunting the law if they think they can “keep the lid on.”

What’s New in the Data Breach World?
The Ponemon Institute’s 2011 Cost of Data Breach Study found that data breaches cost organizations $5.5 million on average in 2011, a cost of $194 per record exposed ($222 per record if caused by an insider).12 While this is a dreadfully high number, bear in mind that many of the reported data breaches have gone public, some of them involuntarily, and they tend to involve very large corporations, which are far more likely to report breaches than smaller entities.

With respect to smaller businesses, the National Small Business Cybersecurity Study, published in 2012, reported that 87 percent do not have a formal Internet usage policy for employees, 83 percent do not have a plan in place for keeping their businesses cyber-secure, 60 percent do not have a privacy policy in place for keeping customer or employee data secure, and 59 percent have no plan in place if a data breach should occur.13

Another 2011 Ponemon study showed that 90 percent of businesses of all sizes reported a security breach in the preceding year. The majority had multiple breaches. It was striking that the majority didn’t have much faith that they could stop breaches in the future. Seventy-seven percent said the attacks were more sophisticated and severe.14

Companies are beginning to ask themselves not “could it happen?” but “when it happens, how will we respond?”

We are seeing a continuing rise in what are known as “advanced persistent threats” (APTs). A true APT is a very sophisticated and ongoing, long-term attack. After they compromise a network, they often go undiscovered for months. APTs (and this term is often too loosely used when the attack is conventional) typically cannot be defended by keeping patches current, running commercial security products, and a defense-in-depth approach. These attacks are specifically targeted as a rule and often exhibit careful long-term planning, also often using brand new vulnerabilities and obfuscation techniques. With APTs, it is sometimes advisable to let the attack continue while you document it and run counterintelligence on it. Forensic analysis is going to be a key activity, adding to the inevitable financial burden.

In spite of the fact that we know a great deal about how to protect ourselves from things like SQL injections—a code injection technique that exploits a security vulnerability in a website’s software—we simply aren’t doing it.

A new development in 2011 was e-mails that appear to come from your printer, scanner, or all-in-one device. They are a form of attack, using e-mails with false header information to get users to click on the link contained in the e-mail. Author Nelson has received such an e-mail:

From: support@senseient.com [mailto:support@senseient.com]
Sent: Thursday, December 01, 2011 3:21 AM
To: Sharon D. Nelson
Subject: Re: Fwd: Re: Scan from a Xerox W. Pro #6979530
This wasn’t a good scam because she knows her company doesn’t have this kind of device, and no KARINA works with her. But there are more sophisticated versions of these attacks, so beware of the new demon in town.

Verizon’s 2012 Data Breach Investigations Report is alarming. The number of compromised records skyrocketed back up to 174 million after reaching an all-time low in 2010 of four million. In fact, 2011 boasted the second-highest data loss total since Verizon started keeping track in 2004. External agents were responsible for 98 percent of the breaches, with insiders implicated in 4 percent. Fifty-eight percent of all data theft was tied to activist groups. So how do the breaches occur? Eighty-one percent involved some form of hacking, 69 percent used some form of malware, 10 percent involved physical attacks, and 7 percent used some form of social engineering. It is interesting to explore some of the commonalities: 96 percent of the attacks were not highly sophisticated, 79 percent of the victims were “victims of opportunity,” 94 percent of all compromised data involved servers, 92 percent of the incidents were discovered by a third party (often the FBI), and 85 percent of the incidents took weeks (or more) to discover.

While the insider threats appear to be down, bear in mind the case of Matthew Kluger, a lawyer who allegedly stole insider information from the law firms he worked for during a 17-year period. At Wilson Sonsini Goodrich & Rosati, his most recent employer, he got the information from the firm’s document management system. As Law Technology News pointed out in 2011, this underscored three law firm information security challenges:

- The need to balance security with the need to share information;
- The importance of having security policies, with people in place with enough authority to enforce and monitor the policies, updating them as needed; and
- The need to focus on threats from insiders because the tendency often is to focus on external threats and ignore those in the office.

Finally, Information Week reported in 2011 that a recent survey of 300 IT professionals, two-thirds of them working in companies with more than 10,000 employees, showed that 25 percent of them knew at least one coworker who used privileged login credentials to inappropriately access confidential information. Forty-two percent indicated that the IT staff freely shared passwords and access to multiple systems and applications. Twenty-five percent also indicated that at least some of the superuser passwords granting “God” rights to the network were less complex than what was required of end users. A whopping 48 percent reported that privileged account passwords had remained the same for at least 90 days.

While these are big firm statistics, we have no doubt that this sort of sharing, inappropriate access of data, and poor password management are rife in small firms as well. We’ve even seen firms where select individuals have lists of everyone’s passwords, which are set never to expire.

The government isn’t doing any better than the private sector. The U.S. Government Accountability Office released a report in 2011 acknowledging that there has been a 650 percent increase in malware infections and other security incidents over the past five years.
The Bad Rap Law Firms Get on Information Security

Security consultants consistently report that law firms are “stingy” about spending money on data security and lag far behind their corporate counterparts. Only at the largest firms does one find security specialists. Laws firms in general, and small firms in particular, are not very likely to have vulnerability assessments done. If they do have an assessment done, they often don’t follow the best practice of repeating the assessments at regular intervals. Firm-wide encryption is almost unheard of.

We forget how our mobility has opened up new vulnerabilities. Flash drives, tablets, smartphones—all are easily lost or stolen, yet most lawyers do not encrypt these mobile devices. Sadly, they do not even go to the trouble to have a password or personal identification number (PIN) on their devices.

Social media sites have become a wonderful place for criminals and business espionage experts to set up shop. Even developers for social media sites have been found with their hands in the cookie jar. And yet, we find very few firms with social media policies, training about the safe usage of social media, or implementing technology that might intercept malware before it is installed on the network.

Engagement letters should note that security cannot be guaranteed and advise clients not to send sensitive information electronically. Unfortunately, we rarely see that sort of language used by solos and small firms.

A law firm data breach that made the papers. On October 10, 2011, the press reported that the Maryland law firm of Baxter, Baker, Sidle, Conn & Jones had lost the medical data of 161 patients in a malpractice suit. 19 This was especially significant because it is so rare to hear of law firm data breaches—understandably, law firms are loathe to have such stories become public. So how did this one come to light? The Baltimore Sun obtained a copy of one of the notifications sent to the patients.

Here’s what happened: One of the law firm’s employees brought home a hard drive containing backup data—this was the firm’s method of ensuring that it had an off-site backup. She took the Baltimore light rail system home and—you guessed it—left the drive on the train. Though she returned just a few minutes later, the drive was gone. And yes, the drive was unencrypted.

In any event, it should be clear that traveling with unencrypted backup data is a very bad idea. The firm has begun encrypting its data and is looking into off-site data storage.

State Laws Protecting Personal Data

As we stumble toward a federal data breach law—a process that has taken years—the states have taken matters into their own hands. There are numerous state laws covering security requirements and breach notification. 20

Forty-six states have breach notification laws. Generally, these require that an entity which reasonably believes that there has been a breach involving unencrypted data acquired by an unauthorized person must provide notice to the affected persons.
Forty-nine states have security freeze laws, allowing a customer who has been or believes he or she will be a victim of identity theft to request that a consumer reporting agency place a “freeze” on his or her credit report, blocking any unauthorized access to it.

Thirty-five states have Social Security protection laws that dictate how Social Security numbers may be used or displayed.

Twenty-four states now mandate the secure disposal of personal information in paper and electronic records.

Almost all state laws exempt encrypted information from their personal information breach notice requirements. Several states have laws that require “reasonable security” or its equivalent for personal information. Massachusetts and Nevada have implemented much more stringent security laws that require the encryption of personal information, and such requirements may represent a trend. Washington also has some express encryption requirements. The Massachusetts law is particularly important for attorneys in all states to understand, because it applies extraterritorially to personal information about Massachusetts residents in a database in any state.

Spear Phishing—and a Data Breach Avoided

Spear phishing is targeted phishing. It is more likely to be successful because it often appears to come from someone you trust and the subject line is one designed to engage the recipient. For instance, it might say, “Check this out—you’re quoted in this article.” An appeal to ego is often successful. Once in, the perpetrators will look for administrator accounts and the accounts of managing or senior partners to allow them to move freely within the larger network. In a smaller firm, the e-mail’s subject line might well read, “Referring a case to you”—that would certainly be appealing in these uncertain economic times.

In 2010, the Los Angeles-based firm Gipson Hoffman & Pancione survived an attempted spear phishing attack. The firm had filed a $2.2 billion copyright infringement suit on behalf of CYBERsitter LLC. Shortly thereafter, the firm noted a dramatic increase in suspicious e-mails. The e-mails appeared to be sent from lawyers at the firm and included a message requesting the recipients to open an attachment. The firm’s internal investigation revealed that the attachment contained malware which appeared to come from China.

We can never say enough about the value of training, and training saved the firm from making an error in this case. Attorneys and support staff had been warned to be on the lookout for suspicious e-mails after the suit was filed because the suit accused the Chinese government and several companies of stealing code from CYBERsitter’s Internet filtering program. No one clicked on the attachment, so no malware bomb was detonated.

A new kind of spear phishing was dubbed “whaling” in IBM’s X-Force 2011 Mid-Year Trend and Risk Report. Whaling specifically targets “big fish,” or high-level personnel with access to critical data. The cybercriminals research the “whales” online—usually through social media—and are able to construct messages to people that genuinely appear to come from, say, their boss, which dupes them into clicking on a malicious link. It’s an effective harpoon and gaining traction with the bad guys.

A Nasty Law Firm Data Breach

Another law firm was not so lucky. In 2008, security firm Mandiant discovered that the law firm’s network had been breached for more than a year after the law firm was tipped off to the
breach by law enforcement. We don’t know how law enforcement knew, but more and more, we are seeing businesses warned by authorities, which is interesting.

The law firm could not be named due to Mandiant’s confidentiality agreement, but Mandiant stated that the firm was involved in litigation involving China, common in many breaches in spite of the Chinese government’s many protestations of innocence when the words “state-sponsored hacking” come up. The intruders at the law firm were able to obtain more than 30 sets of user credentials and harvested thousands of e-mails and attachments from mail servers; they also had full access to all servers and computers on the network for an extended time. The fact that this could happen to a law firm should give lawyers a serious case of the willies.

**OK, I’m Convinced—What’s Next?**

First, understand how data breaches happen. Here are the most common ways:

- Devices with unencrypted data are stolen or lost.
- Security patches (updates to address security vulnerabilities) are not installed.
- Lawyers and staff are not trained about social engineering. One example is where someone pretends to be your IT provider and needs an employee’s ID and password to “fix something.”
- Malware comes in via an attachment or through social media (this would include spear phishing).
- Hackers, cybercriminals, and even nations find vulnerability in your network.

Since the old, innocent days of script kiddies, we now have more sinister types trying to get your information, and their skill set has vastly improved along with the tools available. Also, our networks are becoming more interconnected and complex all the time. As Philip Reitinger, the director of the National Cybersecurity Center in the Department of Homeland Security, has said, “complexity is the enemy of security.” As he further pointed out, if someone really wants your data, he or she stands an excellent chance of getting it.25

The Department of Defense reports that its computers are probed hundreds of thousands of times each day. Now your law firm probably isn’t probed that often, but rest assured that it is being probed. Even the power of the cloud can be used to automate the probes.

Here’s another reason to be wary from Alan Paller, the director of research at the SANS Institute: “If I want to know about Boeing and I hack into Boeing, there are a billion files about Boeing. But if I go to Boeing’s international law firm, they’re perfect. They’re like gold. They have exactly what I’m looking for. You reduce your effort.”26

Once you have an understanding of how data breaches occur, the next step is to evaluate your firm’s vulnerabilities. Then devise and implement a security policy and plan. Remember that a successful plan involves training all employees, both initially and periodically. (See “Information Security Program Checklist.”)

Despite a good security plan, at some point your data may be compromised. When an incident is over, sit down and do some serious Monday morning quarterbacking. You may have policies or procedures that need to change. Whatever your incident response plan, it probably did not wholly survive first contact with the enemy.

Never think that you can handle a data breach without expert involvement. Only an information security specialist can truly do that, which is one reason that we haven’t included a
complicated set of technical instructions here. For one thing, they’d be obsolete as soon as written; and for another, they would constitute a book in and of themselves.

Secure Passwords: The Rules Have Changed

Passwords might seem a tired subject to some, but the rules of the security game have changed—and it is high time to say goodbye to those wimpy, eight-character passwords. If you are using less than eight letters, shame on you! Even in 2011, *PC Magazine* reported that the top five passwords were “password,” “123456,” “12345678,” “qwerty” (the top alphabet row on the keyboard, in case you’ve never noticed), and “abc123”; the oddly plaintive “letmein” was number eight. Not strong, not creative, and an invitation to a breach.

*Georgia Institute of Technology report.* The top five passwords listed above are dreadful of course, but even those who were using strong eight-character passwords received a shock when it turned out that those passwords are now insecure. According to a report published by the Georgia Institute of Technology, it is time to move to 12-character passwords. In essence, institute researchers were able to use clusters of graphic cards to crack eight-character passwords in less than two hours. And trust us, if researchers are doing this, so are the cybercriminals of the world.

The researchers discovered that, when they applied the same processing power to 12-character passwords, it would take 17,134 years to crack them. Cybercriminals, even when highly motivated, are going to bypass 12-character passwords—there are just too many folks out there with less secure passwords asking for their security to be violated.

**Lawyers and passwords.** For many years, we have lectured about passwords to audiences of lawyers. In the beginning, it was very frustrating, as lawyers wanted “instant on” information and were unwilling to take passwords very seriously. This is still true in the case of smartphones. Consistently, when we poll lawyer audiences, more than half do not have a PIN on their smartphone. That’s fine until you lose your phone, which is a tremendously common experience. Now the person that finds your smartphone also has “instant on” access to all your data. Not a terribly effective way to safeguard your confidential data.

**Passphrases as passwords.** In response, over the last few years, we have joined others who lecture on security and recommended the use of full sentences or passphrases as passwords. They are so much easier for all of us to recall. “I’m sick of Lindsay Lohan!” is simple enough to remember and complex enough to confound a would-be password cracker. Using characters that are nonletters helps add to the complexity and therefore to your security. The English alphabet contains just 26 letters, but there are 95 letters and symbols on a standard keyboard. “Mixing it up” makes it even more difficult for cybercriminals to break your password.

Some, including Microsoft, will argue that users should not use real words or logical combinations of letters because they may be guessed by a “dictionary attack” using a database of words and common character sequences. Maybe, but we think that is overkill unless you’re dealing with national security data or the formula for Coca-Cola®.

The research used at Georgia Tech was a “brute force” attack, meaning that they simply tried all possible combinations of characters. The computer graphics cards they deployed are very cheap and easily programmed to perform these sorts of computations. We have software in our forensics lab that will natively use the GPU (Graphics Processing Unit) to attack passwords, so the tools are freely available. The processors in the cards all run simultaneously, working to crack the passwords. Amazingly, these processors, running together, now have the processing power of what we used to call “supercomputers.”
Remembering and storing your passwords. Perhaps the greatest problem is remembering all these passwords. One solution is to use an encrypted flash drive such as the IronKey, which includes a password “vault” application that remembers all the characters for you. This has been our solution, which is great—until we forget the IronKey. We can only sigh remembering how many times that has happened; fortunately we’ve always been in the same city as the IronKey. We haven’t managed to lose our IronKeys yet, but as small as they are, that would also be easy. There is an insurance policy—you can store your passwords (encrypted) on the IronKey site. But you can sense that there is a nuisance factor here.

There are websites that will store your passwords for you, but then you must trust the security levels (and employees) of that website.

Particularly dangerous are social media passwords, which are often used to log in all over the Web. Adding to the danger is the fact that third-party applications regularly require you to turn over your social media ID and password so that they can have interaction between, say, Facebook and the popular applications Mafia Wars and Farmville. This makes things easy for the user, but now a cybercriminal with a single set of credentials may be able to access multiple sources of information.

For $19.99, you can turn to a product like eWallet (www.iliumsoft.com/site/ew/ewallet.php), which will store your passwords in encrypted format and allow you to sync access to it from multiple devices, including smartphones (be sure to check that yours is supported). This may be the best solution currently available for busy lawyers. Author Simek uses eWallet as a backup (synced to the Android smartphone) to his IronKey. With a 30-day free trial, it’s hard to go wrong. There are similar products out there, but research them carefully before selecting one. Most have been tested by independent sources—your best way of screening software because all vendors will trumpet their products as “the” solution to your problems.

Is there a way to store passwords on your own system securely? Well, it will help considerably if you store your passwords in a Word document or Excel spreadsheet that is itself password protected. This means that the data will be stored in encrypted format if you have Office 2007 or later. You still need to make sure that the password you use to protect the file is very strong and not the name of your pet cat.

So what if you are asked, while browsing the Web, if you’d like to store your ID and password on the computer being used? Don’t do it. If—however it happens—your machine is compromised or someone who has the keys to your network gets on your computer, you’ve given someone else the power to “be you” on any site where you’ve asked to have the ID and password stored.

Do you need 12-character passwords to access websites? For anything important, of course. You sure wouldn’t want to access your bank, stock market, or retirement account without a strong password. Ditto for anywhere you shop because many of us save credit account information on the site so that we can make purchases quickly. And for heaven’s sake, don’t use the same ID and password on different sites—once one is compromised, so are the rest if you take that perilous route.

A Conversation with a Law Firm Security Specialist
Can we ever get law firm data properly protected from breaches? To answer the question, authors Nelson and Simek interviewed their friend and colleague Matt Kesner, the CIO of
Fenwick & West LLP, a West Coast law firm representing high tech and bio-tech clients. Matt has “walked the walk” when it comes to security and protecting data.

Is the data at a law firm really different or are there “special” considerations when dealing with security within a law firm? Matt suggested that there are a lot of tensions at play within a law firm. There’s always the tension between IT professionals and end users. The end users are more difficult to tame and are more independent than most other users. They don’t necessarily want to comply with the stated policies and procedures, thereby making security a more difficult task. Also, they tend to be driven by what the client wants, which may be in contradiction to the security procedures of the firm.

As we’ve previously discussed, the press hasn’t really identified many data breaches that have involved law firms. Because law firms are very much reputation based, they are not all that willing to publicize any data breach that may have occurred. Current data breach laws have changed that practice, but we still don’t hear of many specifics concerning law firms. Matt acknowledged that there have been two breaches at his own firm. His advice for security is to learn lessons from breaches so you can avoid a recurrence—at least a recurrence of the same sort of attack. Fortunately for Matt’s firm, the security incidents did not involve access to their network. Both occurrences involved their website, which was hosted externally.

We are aware of some other firms being compromised, primarily through mobile devices and unprotected laptops. At a minimum you should have a lock code on your mobile device and the drives on laptops should be fully encrypted. Matt’s excellent advice is, “When in doubt, encrypt it.”

Not to scare our readers (OK, maybe just a little), but Matt confirmed that law firms are seeing an increase in hacking attempts. Reviews of his own firm’s logs show repeated “door rattles” and attempted infiltration of the network. They are being probed a lot more often, are tested with various scripts being used to determine vulnerabilities, and have experienced a higher proportion of successful malware and phishing attacks against their users.

Many attacks appear to be originating from China, which is consistent with our experiences gleaned from security investigations involving these attacks. Our own government has cautioned us that every cell phone and smartphone that goes into China has spyware downloaded on it by the Chinese communications infrastructure. This spyware pretty much has unfettered access to the data that you are sending and receiving even if it is encrypted in transit. Another concern is bringing laptops to China. Matt advised us to weigh the laptop before and after taking it to China, as many times hardware monitoring devices will be installed in the laptop itself. He also suggested taking a disposable cell phone when traveling to China. Many in the security field have stated that we are seeing activity from China’s “C-level” (rookie) hackers because law firm systems are fairly easy to penetrate. China isn’t wasting the efforts of their “B-level” or “A-level” teams when attacking U.S. systems. Essentially, China’s entry-level hackers are practicing on U.S. law firm networks before “graduating” to more advanced hacking activities. Matt told us that Chinese students actually take hacking classes and hack Western websites as part of their homework. Pretty scary stuff.

Increased usage of the Internet, voluminous amounts of data, and the sharing of that data for legitimate purposes has made the task of security even more difficult. There are many more attack points as the data grows and reaches out to many more parties as part of our normal business activities. Matt cautioned us to be wary of USB flash drives that we obtain at conferences because they may be infected with malware such as the Stuxnet virus.
We queried Matt if there really is a fix for the security state that we are currently observing. The answer, as you might have guessed, is that there is no silver bullet for security. His primary advice is to partner with a trusted security advisor and be prepared to budget some funds for security.

**Conclusion**

Security threats to attorneys and law firms are real—attacks on law firm data are occurring and will continue. Attorneys have to understand the risks and implement and maintain reasonable safeguards to protect against them, including assistance from security and IT professionals when necessary. Initial and ongoing training and security awareness programs are critical. Constant vigilance is also required because the security risks of tomorrow will be different from those we see today. Sadly, law firm information security has become a game of Whac-A-Mole. Knock two security threats down and three more appear. Clearly, the days of attorneys and law firms ignoring data security are—and ethically must be—over.

**Notes**

6. Id.
11. HEALTHCARE INFO. & MGMT. SYS. SOC’Y, 5TH ANNUAL HIMSS SECURITY SURVEY 21–22 (2012), available at http://himss.files.cms-plus.com/HIMSSorg/content/files/2012_HIMSS_SecuritySurvey.pdf (finding that hospitals (18 percent) were more likely to report an instance of medical identity theft than were physician practices (6 percent)).


21. MASS. GEN. LAWS ch. 93H; 201 MASS. CODE REGS. 17.00; NEV. REV. STAT. §§ 603A.210 et seq.

22. E.g., WASH. REV. CODE §§ 41.05.042 (health information), 19.255.010–.020 (payment card data).


26. Id.


Information Security Program Checklist

- **Risk Assessment**
  - Inventory of information assets
  - Identify duties to safeguard (ethics, common law, contracts, statutes/regulations)
  - Evaluate need for outside security resources
  - Identify internal and external threats
  - Identify and evaluate current safeguards
  - Identify reasonable safeguards to address identified risks

- **People**
  - Assign responsibility for security program
    - Person(s) in charge
    - Responsibilities of all users
  - Training
    - Initial, including new employees
    - Periodic
    - Promote constant security awareness
  - Monitor compliance
  - Enforcement

- **Policies and Procedures**
  - Comprehensive written program/policy
  - Screening of new employees
  - Blocking terminated/resigned employees
  - Management for third parties given access to confidential information
  - Limit access to confidential data to those with need to access
  - Secure disposal—paper and electronic
  - Training
  - Supervision and monitoring
  - Incident response, including notification
  - Review safeguards periodically and with changes in risk, threats, and technology
  - Periodically evaluate need for outside security resources (including security audits and penetration testing)

- **Technology**
  - Physical security of confidential information and network resources
  - Secure configuration (network and endpoints)
  - Firewall and network appliances
  - Security software: current version + update
  - Patch management (network and endpoints)
  - Authentication and access control
    - Manage password/passphrase age and complexity
    - Change all default passwords
    - Block access after multiple failed attempts
    - Timeout after inactivity (automatic logoff or screensaver requiring password)
    - Strong authentication for remote access (two-factor best)
  - Encryption of confidential data on laptops and portable media
  - Encryption of confidential data transmitted over the Internet or wireless networks
  - Monitoring and logging
☐ Equipment or vendor for secure disposal