VIII. Legal Ethics Update

Sara Anne Hook, M.B.A., J.D.

A. Mobile Device Use and Client Confidentiality

The same ethical rules apply in the mobile world as they do in the in-person world. For example, ABA Model Rule 1.1 on Competence, Comment 8, Maintaining Competence states that:

> [8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1.html, accessed 6/22/17.)

Likewise, the ABA Model Rules of Professional Conduct as well as the Indiana Rules of Professional Conduct stress the lawyer's duty to safeguard client confidentiality, including Rule 1.6. Note that the duty of confidentiality is owed to both former (Rule 1.9, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_9_duties_of_former_clients.html, accessed 6/22/17) and prospective (Rule 1.18, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_18_duties_of_prospective_client.html, accessed 6/22/17) clients.

Mobile devices present special risks to client confidentiality. One of the major reasons for this is the percentage of laptops, tablets, cellphones and other devices, such as flash drives, that are lost or stolen. Unfortunately, many lawyers do not take the simple steps necessary to safeguard these devices or the information stored on them. For excellent information and practical recommendations about issues related to information security, lawyers are advised to purchase *Locked Down: Practical Information Security for Lawyers*, 2nd edition (S.D. Nelson, D.G. Ries and J.W. Simek, ABA, 2016. This is

the textbook that I use for the course I teach on cybersecurity every Spring semester which is one of the required courses for the legal informatics certificate. In addition to chapters on encryption, authentication and authorization and security tools and services, the authors have specific chapters that cover each type of mobile device, including desktops, laptops and servers, smartphones and tablets and portable storage devices. Additional chapters cover what do to with digital copiers, scanners and fax machines, voice communications and secure methods for disposal. Lawyers should also consult the website for Sensei Enterprises, Inc., (https://senseient.com/, accessed 6/22/17) which features articles, blogs, podcasts, YouTube videos and other helpful resources on security, information technology, electronic discovery and digital forensics. I subscribe to the free article delivery service. It is an excellent way to stay current on these important issues as well as to obtain practical recommendations on how to practice law more securely and ethically.

Chapter 11 in *Locked Down: Practical Information Security for Lawyers*, 2nd ed. is devoted to managing and securing smartphones and tablets. As stated on page 143, "[d]evices that were designed as consumer products must now be managed and secured in a business environment." The authors note that smartphone users are exposing their employers to security threats in major ways. Wearable devices will present new challenges. However, as the authors assert, "[t]here is a growing consensus that the use of smartphones and tablets, if done the right way, can be accomplished safely and will greatly benefit businesses and professionals." According to the *2015 American Bar Association Legal Technology Survey Report*, 90% of responding lawyers reported that they use smartphones for law-related tasks and almost 50% reported that they use tablets. The International Legal Technology Association's 2015 survey also shows a substantial and increasing use of smartphones and tablets.

Note the discussion of the duty to safeguard client information on pages 144-145, embodied under Rule 1.1 on competent representation and ethics opinions from California and Pennsylvania on the use of technology to transmit or store confidential

client information and the lawyer's use of cell phones and laptops as part of cloud computing, respectively. The authors assert that the same kind of attention should be given to the selection and use of smartphones and tablets, although it would appear that lawyers have been using these devices without evaluating the risks and without first addressing security measures.

As indicated on page 145, many security breakdowns are caused by lack of attention to risks and appropriate security measures. They suggest that when purchasing a new smartphone, tablet, laptop or other mobile device, users should consider security (both native and available add-ons) as part of the selection process. Constant security awareness is essential – every day, every time that mobile technology is being used. The basic steps for secure setup and use of mobile technology are provided on pages 146-147:

1. Review and follow the security instructions of the device's manufacturer and carrier.
2. Maintain physical control of the device.
3. Set a strong password, passphrase or personal identification number (PIN).
4. Set locking after a set number of failed attempts.
5. Set automatic logoff after a defined time of inactivity.
6. Encrypt confidential data on the device and any storage cards.
7. Provide for protection for data in transit, including secure, wired and wireless connections.
8. Disable interfaces that are not being used, such as Bluetooth or WiFi.
9. Enable remote location, locking and wiping of a lost device.
10. Consider using third-party security applications (antivirus, encryption, remote locating, wiping, etc.)
11. Back up important data.
12. Do not "jailbreak" or "root" a smartphone. These unlock a device, including its security controls.
13. Promptly apply updates to the operating system and apps – they often address security issues.

In addition to secure setup for smartphones and tablets, the authors recommend some additional measures for **secure use**:

1. Limit confidential data on the phone or tablet to only what is necessary. Don't put this data on your phone or any mobile device just because you can.

2. Be careful in selecting and installing applications. This is particularly important with Android for apps obtained from sources other than Google Play.
3. Pay careful attention to permissions given to apps (what the app can access) and the Terms of Service (what the app or service may do with the data it accesses, including sharing it with third parties).
4. Configure web accounts and remote access to use secure connections – https or virtual private networks (VPN).
5. Don't use public wireless clouds for confidential use – or at a minimum, take appropriate precautions.
6. Don't open suspicious emails or follow suspicious links in emails and text messages.
7. Be careful with attachments – they sometimes contain malware.

The authors have been long-time advocates of encryption on nearly all types of communication, which is considered by some commentators as a "security no-brainer."

The authors devote the remainder of Chapter 11 to additional information on security considerations for smartphones and tablets. Note especially the information on Blackberry, iOS and Android, particularly the discussion of malware. As they report on page 150, NSA has developed a high-security version of Android called the Security Enhanced (SE) Android. Some of its features are being incorporated into the Android operating system by Google. Android devices using Android SE and strong controls are reportedly being produced for the federal government for military and national security use. The authors examine the offerings from Silent Circle and Open Whisper Systems. Mobile Device Management (MDM), which is evolving into Enterprise Mobility Management (EMM), is another option; a number of vendors have products and services for MDM. As stated on pages 150-151, "[i]n an enterprise environment like a law firm, mobile device management (MDM) is necessary in addition to the security measures applied to each device." MDM includes centralized control of mobile devices, such as inventory, policy development, password management, authentication and authorization, enforced wiping or locking, strong encryption and timeout after a period of inactivity, to name but a few.

Portable storage devices are covered in Chapter 12 of *Locked Down: Practical Information Security for Lawyers*, 2nd ed. The attributes that make portable storage

devices useful also make them very dangerous from a security perspective. One survey reported that 70% of data breaches resulted from the loss or theft of off-network equipment (laptops, PDAs and USB drives). Note the recent data breach report from a law firm in Maryland that lost an unencrypted portable hard drive with medical records of patients. The procedure for backing up the law firm's data was questionable, especially since the drive was not even encrypted. As the authors point out, massive amounts of data can now be stored on very small devices, which can present considerable risks if lost or stolen. The authors provide a list of security measures for portable media on page 154. As indicated on page 154, because of a major security breach involving information on 28 million veterans, the Office of Management and Budget issued security guidelines for federal agencies which include a requirement for encryption of all data on laptops and portable devices, unless the data is classified as "non-sensitive". The authors recommend that this information security standard be followed by everyone. As they state on page 154, "[l]ike hard drives in computers, portable drives, both USB flash drives and external hard drives, can be protected by built-in encryption or software encryption." Software encryption can be preinstalled on the drive or added by Windows, Apple's OS X or by third-party encryption products.

The authors provide a discussion of encrypted USB drives on pages 154-157. Individual USB drives are available with built-in encryption, such as CMS Secure Vault, Kanguru Micro, Kingston Data Traveler and from SanDisk Cruzer. Thumb drives with encryption look the same as unencrypted thumb drives (see Figure 12-1, a CMS Products CE Secure Vault flash drive), but encryption can be enabled by simply following the manufacturer's instructions and remembering to back up the encryption key by saving it in a safe location off of the device (see Figure 12-2). The authors caution that you be sure to understand and follow directions when you connect the drive to a computer. Figure 12-3 provides an example of a screenshot of the files on a SanDisk Cruzer Blade flash drive. On any device that is not fully encrypted, it is essential that you store confidential information only in the encrypted portion. IronKey, by Imitation, is a favorite of the authors; several of the models include a secure password management application and

may allow for secure Internet browsing. The authors provide a discussion of some encrypted external hard drives, operating system encryption of portable drives and encryption software on pages 157-158. At the end of Chapter 12, the authors emphasize that, as with laptops and desktops, it is best to actively manage encryption for portable storage devices centrally on an organization's own server. They conclude that portable storage devices present a high-security risk that must be managed, especially when these devices are used by lawyers and contain confidential client information.

B. Ethical Email Practices

Email is still the most common form of communication, particularly for most clients. Yet email is fraught with ethical issues, particularly in terms of client confidentiality, but also its very informality and ubiquitous-ness tends to mean that people are not as careful about what they say in an email message and how they say it nor who receives it, the fact that it is likely distributed widely or that it nearly is always preserved in some fashion, somewhere. Some of the easiest ways that client confidentiality is put at risk through email is over-use of the Reply All feature (without looking to see who else is on the distribution list) or the "helpful" feature of email systems that automatically begin to fill in the recipient information with only the typing of a couple of letters.

Email security is the focus of Chapter 18 in *Locked Down: Practical Information Security for Lawyers*, 2nd ed. The authors note that email is an everyday form of communication - it is fast, convenient and inexpensive – but it presents serious security risks with respect to confidentiality, integrity and availability. The authors remind us that lawyers have an ethical duty to safeguard information, as embodied in the ABA Model Rules and the various state Rules of Professional Conduct, such as Rule 1.6 on confidentiality. As noted in Comment 19 to Model Rule 1.6, lawyers must take "reasonable precautions" to protect electronic communications. Remember that under Rule 5.3, the lawyer retains ultimate responsibility for the activities of employees as well as third-party vendors, contractors and consultants. Although several formal ethics

opinions indicate that encryption of email is not mandatory, the authors caution that these opinions contain qualifications that limit their general pronouncements and there may be duties through common law (previous court decisions), contracts and agreements and regulatory requirements. However, note that recent ethics opinions from California, Pennsylvania and Texas have concluded that encryption of email may be required in certain circumstances.

The authors identify and discuss nine areas of risk in the use of email by lawyers and others on pages 195-196:

1. Lack of confidentiality.
2. Authenticity.
3. Integrity.
4. Non-repudiation.
5. Misdirection or forwarding.
6. Informality.
7. Permanence.
8. Malware, such as viruses, worms and spyware.
9. Inappropriate instant responses.

The authors suggest that some of these risks can be reduced or even eliminated by using proper practices, procedures and technology (such as encryption or authentication). As a deltiologist (postcard collector), I love the comparison of email to postcards, especially postcards written in pencil. The lawyer's duty is to use reasonable and competent safeguards, which may include encryption (see California Formal Ethics Opinion No. 2010-179 in Appendix D). The authors provide an explanation of encryption on pages 197-198. As indicated on page 197, the term encryption generally means both encryption and authentication processes used in combination to protect email. Encryption protects the confidentiality of email while authentication (signing) identifies the sender of an email message and verifies its integrity. The authors explain how to use encryption in Outlook 2013 and 2016, with the Security Properties dialog box shown in Figure 18-1. As an alternative, you could select the Encrypt icon in the Permission section of the Options tab, illustrated in Figure 18-2.

Digital authentication of email generally uses a key pair. The authors describe the process for doing this in Outlook 2013 and 2016 on pages 198-199. As they observe on page 199, the challenging part is obtaining key pairs, exchanging public keys and setting keys up in the email program for encryption. The management and exchange of keys are the major reasons why people avoid using encryption. Keys are available from commercial public key authorities such as those mentioned on page 199. Another form of email encryption is Transport Layer Security (TLS) encryption, which protects email in transit, as discussed on pages 199-200. Secure email is available from managed messaging service providers like DataMotion, Mimecast, HP Voltage and Zix Corp. The authors describe these services as inexpensive and easy to use, but that you will require assistance with initial installation and configuration. As they note on page 200, they are seeing more law firms implement this kind of encryption because of the ease of use and low cost.

An alternative to encryption is to protect confidential information by putting it in a password-protected attachment rather than in the body of an email message (see New Jersey Opinion 701), with some suggestions for how to do this provided on pages 200-201. Note that this approach to protecting the confidentiality of email attachments is not as secure as the other methods, particularly if users choose weak passwords. The final paragraph in Chapter 19 of *Locked Down: Practical Information Security for Lawyers*, 2nd ed. is very important. Commentators strongly recommend that the lawyer discuss the issue of how to share (and how not to share) confidential information with their clients and even to have clients agree in writing to the method or methods of communication that will be used during the representation.

C. Attorney Duties to Non-Clients Online

There are a number of duties outlined in the Indiana Rules of Professional Conduct (http://www.in.gov/judiciary/rules/prof_conduct/prof_conduct.pdf, accessed 6/22/17) with respect to individuals who are not clients and these duties must be carefully considered in the 21st century. Some of these duties are:

- Rule 1.14. Client with Diminished Capacity
- Rule 1.16. Declining or Terminating Representation
- Rule 4.1. Truthfulness in Statements to Others
- Rule 4.2. Communication with Person Represented by Counsel
- Rule 4.3. Dealing with Unrepresented Persons
- Rule 4.4. Respect for Rights of Third Persons

Unfortunately, social media and the ease of other technology-facilitated communication methods mean that many people are confused about whether and when a relationship or connection has been made. In a paper-based world, the cases involving a person's belief that he or she was represented by counsel were nearly always decided in that person's favor as opposed to the lawyer's view that there was no lawyer-client relationship established nor that the lawyer had agreed to the representation. The court's view was that the lawyer was in the best position to clarify the relationship – or lack thereof. Thus, declination letters were usually advised. In the virtual world, people may think that contacting a lawyer via email, through a website or through a third-party directory or matching system may mean that he/she now "has a lawyer." To avoid this situation, it is advisable to include disclaimers on all websites, blogs and other forms of electronic communications as well as to provide the same language at the end of emails. Lawyers should also be judicious in all communications so as not to give the appearance of providing legal services or advice. Here is a sample disclaimer that a colleague uses at the end of his email messages:

> This message and any attachments are from Redding Law and are covered by the Electronic Communications Privacy Act (18 U.S.C. 2510 et. seq.). This message, plus attachments, may contain legally privileged or confidential information intended only for the addressee. If you are not the addressee, of if this message has been addressed to you in error, you are not authorized to read, copy or distribute this message or any attachments. We ask that you delete this message and attachments (including all copies) and notify us by return email or phone

(317) 426-1316. Delivery of this message and any attachments to any person other than the intended addressee is unauthorized and is not intended in any way to waive any confidentiality or privilege. Additionally, mere receipt of this email does not, on its own, create an attorney client relationship and no such relationship should be inferred.

Likewise, the disclaimer on the website of SmithAmundsen (http://www.salawus.com/disclaimer.html, accessed 6/22/17) is particularly extensive and includes the following provisions:

> ***Portions of this website may constitute attorney advertising. The choice of a lawyer is an important decision and should not be based solely upon advertisements.***
>
> ***No Attorney-Client Relationship Created by Use of this Website.*** This website is not intended to create an attorney client relationship. Neither your receipt of information from this website, nor your use of this website to contact SmithAmundsen (hereinafter "the Firm") or one of its lawyers creates an attorney-client relationship between you and the Firm. You will become a client of the Firm only if and when you sign an engagement agreement setting forth the scope of the Firm's engagement, the fee arrangement and other relevant matters. The Firm does not accept a new client without first investigating possible conflicts of interests and obtaining a signed engagement letter. (The Firm may, for example, already represent another party involved in your matter).
>
> ***No Legal Advice Intended.*** This website includes general information about legal issues and developments in the law and is not intended to be legal advice, nor should it be construed as legal advice, on any subject matter. Such materials are for informational purposes only and may not reflect the most current legal developments. Legal advice cannot be given without full consideration of all of the relevant information relating to your particular set of facts or circumstances. No recipients of content from this site, client or otherwise, should act or refrain from acting on the basis of any content included on the site without seeking the appropriate legal or other professional advice from an attorney licensed in the recipients' state. SmithAmundsen LLC expressly disclaims all liability with respect to actions taken or not taken based on any or all contents of this site.
>
> ***No Confidentiality.*** Do not use this website to provide confidential information about a legal matter of yours to the Firm. Please communicate with one of the Firm's lawyers in person or by telephone. Use of this website, filing in a form on this website, or sending an unsolicited email to the Firm or any of its lawyers does not make you a client of the Firm or even a prospective client of the Firm. The

Firm has no duty to maintain the confidentiality of any unsolicited information sent by you.

As of this writing, revisions to Indiana Rules of Professional Conduct 7.1 and 7.2 were being forwarded for possible approval. The major revision would be to Rule 7.1, which would eliminate the itemized list of information that is considered inherently "misleading" and thus not currently permitted as part of communications concerning a lawyer's services. Lawyers do need to read the revised section 2 of this Rule carefully as well as the new sections 3 and 4. It is hoped that, if approved, the simplification of Rule 7.1 will provide greater clarity and comfort to law firms about the kinds of information that can be featured on websites, blogs and other social media. At the same time, allowing potential clients to have access to such information as presented in statistics, testimonials and endorsements, comparisons for services and dramatizations is more in line with the kinds of information that typical consumers seek when making decisions about other products and services, including professional services.

D. Virtual Law Office – Ethical Guidance

All of the lawyer's ethical responsibilities are still in force, whether the lawyer has a physical law office, a virtual law office or a mixture of both. One risk that is increasing exponentially, no matter how or where the lawyer practices, is security. The authors of *Locked Down: Practical Information Security for Lawyers*, 2nd ed. sound a clear alarm in the very first chapters.

The Introduction to *Locked Down: Practical Information Security for Lawyers*, 2nd ed. highlights something I have observed over the past few years – what the authors describe as a "veritable revolution" in information security since the first edition of their book appeared in 2012. Of course, high-profile breaches at companies, government agencies and law firms have convinced many people, including lawyers, of the need for more robust information security and privacy practices. Moreover, the revisions to the ABA Model Rules of Professional Conduct require lawyers to be competent in the use of technology and to take reasonable measures to secure information about their clients. As

the authors emphasize on the next page, one of the greatest difficulties with information security is that it is a moving target – and a target that is moving faster and faster each year. Fortunately, there are some guiding principles that remain largely the same. They observe that information security is much more difficult now that we have moved to the Internet, almost universal connectivity and widespread mobility. The term "cybersecurity" focuses on cyberspace and connectivity, but information security encompasses so much more, including the loss, theft and unauthorized physical access of individual computers, servers and mobile devices. It is clear that the authors do not believe that lawyers are doing enough to safeguard information about their law firms and clients, with some sobering information on why this is their opinion. Of course, data breaches and other incidents can happen in spite of reasonable and even robust information security and privacy measures, the authors surmise that the frequency of data breaches at law firms must mean that even reasonable safeguards are not in place. The following may be reasons for this lack of reasonable safeguards:

- Lack of knowledge
- The "it can't happen here" mentality
- Lawyers and law firms (and other organizations) may be considered "soft targets" – having high-value information and weak security
- True information security is expensive
- The need for vigilance never stops

Clients are also demanding more in way of security, which is certainly a motivating factor in the current competitive world of law practice. Information security-savvy clients will factor information security into their decisions about which law firms to work with. On the other hand, the ABA's *2015 Legal Technology Survey Report* indicates that data breaches are increasing, especially in larger law firms. The authors recently published an article indicating that insurance companies are less and less willing to cover information security incidents. People tend to think that information security attacks only come from outside an organization. However, it often an "insider" who intentionally or inadvertently puts confidential information at risk. Given the ethical

responsibilities that lawyers have, it is shocking that law firms would actually hire hackers to glean information about the opponents in a case.

The authors devote Chapter One of *Locked Down: Practical Information Security for Lawyers*, 2nd ed. to looking at what developments are affecting information security in law firms. First, the statistics from the *2015 Verizon Data Breach Investigations Report* indicate the number of breach and security incidents where information was compromised, how quickly this can be done and how often it was the users who provided these opportunities by not following even the most basic security practices, such as taking care with email messages. As the authors observe on page 1, this means that people need ongoing training in safe computing and social engineering. The occurrence of ransomware that encrypts an organization's data and holds it hostage for ransom increased by 4000% in 2014. The authors have advocated the use of encryption as a basic security measure for many years, but here they reveal that of the 237 data breaches reported worldwide by SafeNet in 2014, encryption was in place in only 10.

It is exciting to learn about the plans and activities of the Legal Services Information Sharing and Analysis Organization (LS-ISAO), launched in 2015 with the help of the Financial Services Sharing and Analysis Center (FS-ISAC), considered one of the most mature ISAC/ISAOs. As indicated on page 2, ISACs and ISAOs provide an official mechanism for sharing information about cyberattacks and threats in specific industries, provide a database of threats and vulnerabilities and offer ways for members to learn, interact and collaborate. Among the other industries with ISACs and ISAOs are aviation, the defense industrial base, emergency services, information technology, maritime, nuclear energy, real estate, public transportation, retail, and water utilities. This is especially interesting to me because a number of years ago, the newly established International Legal Technical Standards Organization (ILTSO) circulated the first standards for law firms for security of local networks, cloud services and access devices. I was a member of the Advisory Board of ILTSO and helped write the ethical section of

the standards. We were "pioneers" in those days and received some resistance to our proposed standards, which featured tiers of security measures.

As described on page 3, the Federal Trade Commission (FTC) has brought more than 50 actions related to data security based on its authority to take action against unfair and deceptive business practices, with the ruling by the Third Circuit Court of Appeals confirming this authority in the *Wyndham WorldWide Corporation* case. Similarly, in 2014, the Federal Communications Commission (FCC) imposed a $10 million fine against two telecommunications companies that allegedly stored personally identifiable customer data online without using firewalls, encryption or password protection. The data breach at Target in 2014 happened because of access to the corporate network by an HVAC vendor whose own network was compromised. Thus, vendor management, including their security and restricting their level of access, is now a consideration. Contracts with third-vendors should include employee security training, insurance coverage for data breaches, various warranties, indemnification, and duties to notify and investigate suspected security incidents. The Cyber Information Sharing Act (CISA) was signed into law by President Obama just over a year ago, albeit with a number of concerns reflected in the reactions of the Electronic Freedom Foundation, privacy and industry advocates, computer security specialists, and even the Department of Homeland Security.

Pages 5-6 of *Locked Down: Practical Information Security for Lawyers*, 2nd ed. discuss the information security risk known as spear phishing, regarded as the most effective way to breach a law firm. Of course, we all want to receive good news, such as being quoted in an article or having a new customer or client referred to us. Thus, it is very tempting to open or click on a phony email or attachment. More recently, many phishing attempts are fashioned to look like they come from legitimate government agencies such as courts or the Internal Revenue Service (IRS). One clue used to be improper grammar and spellings – but our authors note that perpetrators have become much more sophisticated and use social media to mine for intimate information to make

the message look real. Ongoing training is essential. Spear phishing points to the ongoing theme that humans are the greatest information security risk and that "social engineering" rather than technology skills are a hacker's best weapon. As indicated on page 6, the FBI warned in 2015 that 7,000 U.S. companies reported $747 million in losses from such attacks since 2013. As defined by Lifewire,

> Whaling is a specific form of phishing meant to target upper managers in private companies. The objective is to swindle the upper manager into divulging the confidential company information on their hard drives. Whaling emails are designed to masquerade as a critical business email, sent from a legitimate business authority with content that is tailored for upper management and usually involves some kind of falsified company-wide concern. (Lifewire.com, https://www.lifewire.com/what-is-whaling-2483605, accessed 6/22/17.)

Perpetrators can easily find information about top executives through the Internet.

Fortunately, as the authors discuss on pages 6-8, the reputation that law firms have had for being "stingy" about investing in information security as compared with their counterparts in other industries is changing, albeit slowly, especially in small firms. Clients may require law firms to complete security assessments that may be as long as 25-60 pages in length. Despite the temptation, for both legal and ethical reasons, lawyers must answer the questions accurately and fully. For the first time since I graduated from law school, I have to submit a Cyber Liability Premium Indication Form as part of my application for malpractice insurance. As reported on page 7, firm-wide encryption is almost unheard of in spite of the new vulnerabilities posed by mobile devices and access. Note that Opinion 648, issued by the State Bar of Texas in 2015, provides several examples of where encryption or other security methods may be appropriate. However, because encrypting email is now so simple and inexpensive, the authors suggest that it could be unethical NOT to use it in many circumstances.

As reported on page 8, large law firms now spend an average of 1.9% of their gross revenues on information security and some are seeking ISO 27001 certification to demonstrate to clients that they are serious about security for their information. On page 8, the authors reveal the most common causes of data breaches – note how many can be

easily addressed by encryption and better training. On the other hand, the risks increase as our networks (including the networks that run a country's critical infrastructures) become more interconnected and complex. It is particularly important to handle a data breach or other information security incident properly. As the authors note at the bottom of page 9, law firms (and other organizations) now have even more incentive to secure their confidential information, especially if it means gaining or keeping a client.

E. Client Access to the File

With more law firms using cloud computing, it is quite possible to allow clients, especially sophisticated clients, to have access to certain pieces and parts of their files. In fact, some clients may want to have a more collaborative role in the case. However, this must be done with great care, particularly as every person with access to a file means an additional risk for a security breach. In addition, there are issues when there is a future dispute about non-payment of fees and the lawyer is withholding the file or the turn-over of the file to successor counsel. Some law firms may allow clients to complete intake forms, using a word processing program or via the web. This not only saves time for the law firm, because the system can be arranged to just import this information into a case management system, but it also gives the client some responsibility for and an something to do for the case.