VIRGINIA BEACH BAR ASSOCIATION

THE ETHICS OF CYBERSECURITY: PRACTICAL AND BUDGET-FRIENDLY TIPS FOR LAWYERS

October 30, 2019
3:00 p.m. to 5:00 p.m.
Wyndham Virginia Beach Oceanfront
5700 Atlantic Avenue
Virginia Beach, VA 23451

DISCLAIMER: The speakers who present at this CLE have graciously agreed to prepare and present material at this CLE session. The views expressed by them are entirely their own, and are not necessarily those of the Virginia Beach Bar Association. The Virginia Beach Bar Association's decision to allow these speakers to present at a CLE session does not constitute an endorsement or recommendation of them by the Virginia Beach Bar Association.

Virginia MCLE Board

CERTIFICATION OF ATTENDANCE (FORM 2)

MCLE requirement pursuant to Paragraph 17, of Section IV, Part Six, Rules of the Supreme Court of Virginia and the MCLE Board Regulations.

Certify Your Attendance Online at www.vsb.org

.

MCLE Compliance Deadline - October 31. MCLE Reporting Deadline - December 15.
A $100 fee will be assessed for failure to comply with either deadline.

Member Name: _____ **VSB Member Number:** _____

Address: _____ **Daytime Phone:** _____

_____ **Email:** _____

_____

City **State** **Zip**

Course ID Number: **VIGG009**

Sponsor: **Virginia Beach Bar Association**

Course/Program Title: **The Ethics of Cybersecurity: Practical and Budget-Friendly Tips for Lawyers**

Live Interactive * **CLE Credits (Ethics Credits):** **2.0** **(2.0)**

Date Completed:_____ **Location:** _____

By my signature below I certify

___ I attended a total of _____ (hrs/mins) of **approved CLE**, of which (_____) (hrs/mins) were in **approved Ethics**. Credit is awarded for actual time in attendance (0.5 hr. minimum) rounded to the nearest half hour. (Example: 1hr 15min = 1.5hr)

___ The sessions I am claiming had written instructional materials to cover the subject.

___ I participated in this program in a setting physically suitable to the course.

___ I was given the opportunity to participate in discussions with other attendees and/or the presenter.

___ I understand I may not receive credit for any course/segment which is not materially different in substance than a course/segment for which credit has been previously given during the same completion period or the completion period immediately prior.

___ I understand that a materially false statement shall be subject to appropriate disciplinary action.

* NOTE: A maximum of 8.0 hours from pre-recorded courses may be applied to meet your yearly MCLE requirement. Minimum of 4.0 hours from live interactive courses required.

_____ _____

Date Signature

This form may be mailed to:

Virginia MCLE Board
Virginia State Bar
1111 East Main Street, Suite 700
Richmond, VA 23219-0026
(804) 775-0577
www.vsb.org

[Office Use Only: Live]

Virginia Beach Bar Assn.

The Ethics of Cybersecurity: Practical and Budget-Friendly Tips for Lawyers

October 30, 2019

Presenters:

Sharon D. Nelson, President, Sensei Enterprises Inc.
snelson@senseient.com

John W. Simek Vice President, Sensei Enterprises Inc.
jsimek@senseient.com

Kellam T. Parks, Parks Zeigler, PLLC
kparks@pzlaw.com

Safeguarding Client Data: Attorneys' Legal and Ethical Duties

David G. Ries

Clark Hill PLC

412.394.7787

dries@clarkhill.com

(Used by the author's kind permission)

April 2019

Contents

Confidential data in computers and information systems, including those used by attorneys and law firms, faces greater security threats today than ever before. And they continue to grow! 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 lost or stolen laptops, tablets, smartphones, and USB drives, as well as inside threats - malicious, untrained, inattentive, and even bored personnel.

These threats are a particular concern to attorneys because of their duties of competence in technology and 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.

Breaches have become, so prevalent that there is a new mantra in cybersecurity today – it's "when, not if" there will be a breach. Robert Mueller, then the FBI Director, put it this way in an address at a major information security conference in 2012:[i]

> I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.

This is true for attorneys and law firms as well as other businesses and enterprises. Consistent with this threat environment, New York Ethics Opinion 1019 warned attorneys in May 2014:

Cyber-security issues have continued to be a major concern for lawyers, as cyber-criminals have begun to target lawyers to access client information, including trade secrets, business plans and personal data. Lawyers can no longer assume that their document systems are of no interest to cyber-crooks.

ABA Formal Opinion 477 (May 2017) (discussed below), describes the same current threat environment:

> At the same time, the term "cybersecurity" has come into existence to encompass the broad range of issues relating to preserving individual privacy from intrusion by nefarious actors throughout the Internet. Cybersecurity recognizes a … world where law enforcement discusses hacking and data loss in terms of "when," and not "if." Law firms are targets for two general reasons: (1) they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client, and (2) the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client.

The ABA's *2018 Legal Technology Survey Report* reports that law firms have been and continue to be victims of data breaches. The *2018 Survey* notes that about 23% of respondents overall reported that their firms had experienced a security breach at some point. The question is not limited to the past year, it's "ever." A breach broadly includes incidents like a lost/stolen

computer or smartphone, hacker, break-in, or website exploit. This compares with 22% in the 2017 *Report*, 14% in 2016, 15% in 2015, 14% in 2014, and 15% in 2013—an increase of 8% in 2017 after being basically steady from 2013 through 2016.

In 2018, the reported percentage of firms experiencing a breach generally increased with firm size, ranging from 14% of solos, 24% of firms with 2-9 attorneys, about 24% for firms with 2-9 and 10-49, 42% with 50-99, and about 31% with 100+. As noted above, this is for firms who have experienced a breach *ever*, not just in the past year.

Security threats to lawyers and law firms continue to be substantial, real, and growing – security incidents and data breaches have occurred and are occurring. It is critical for attorneys and law firms to recognize these threats and address them through comprehensive information security programs. **The greatest security threats to attorneys and law firms today are most likely spearphishing, ransomware, business email compromise, and lost and stolen laptops and mobile devices.**

I. Duty to Safeguard

Attorneys have ethical and common law duties to take competent and reasonable measures to safeguard information relating to clients and also often have contractual and regulatory duties to protect confidential information.

Ethics Rules. Several ethics rules[ii] have particular application to protection of client information, including competence (Model Rule 1.1), communication (Model Rule 1.4), confidentiality of information (Model Rule 1.6), safeguarding property (Model Rule 1.15), and supervision (Model Rules 5.1, 5.2 and 5.3).

Model Rule 1.1: Competence 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, including cybersecurity. It requires attorneys who lack the necessary technical competence for security to learn it or to consult with qualified people who have the requisite expertise.

The ABA Commission on Ethics 20/20 conducted a review of the Model Rules 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 recommendations in this area were adopted by the ABA at its Annual Meeting in August of 2012.

The 2012 amendments include addition of the following underlined language to the Comment to Model Rule 1.1:

[8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, <u>including the benefits and risks associated with relevant technology</u>…

As of March 2019, 36 states have adopted this addition to the comment to Model Rule 1.1, some with variations from the ABA language.

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 a compromise of confidential information relating to the client.

Model Rule 1.6: Confidentiality of Information 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 2012 amendments added the following new subsection (underlined) to Model Rule 1.6:

(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 in litigation, or exposing confidential metadata. Unauthorized access includes threats like hackers, criminals, malware, and insider threats.

The 2012 amendments also include additions to Comment [18] to Rule 1.6, providing that

"Reasonable efforts" require a risk-based analysis, considering the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed and consideration of available safeguards.

"reasonable efforts" require a risk-based analysis, considering the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed and consideration of available safeguards. The analysis includes the cost of employing additional safeguards, the difficulty of implementing them, and the extent to which they would adversely affect the lawyer's ability to use the technology. The amendment also provides that a client may require the lawyer to implement special security measures not required by the rule or may give informed consent to forego security measures that would otherwise be required by the rule.

Significantly, the Ethics 20/20 Commission noted that these revisions to Model Rules 1.1 and 1.6 make explicit what was already required rather than adding new requirements.

Model Rule 1.15: Safeguarding Property requires attorneys to segregate and protect money and property of clients and third parties that is held by attorneys. Some ethics opinions and articles have applied it to electronic data held by attorneys.

Model Rule 5.1: Responsibilities of Partners, Managers, and Supervisory Lawyers and Model Rule 5.2: Responsibilities of a Subordinate Lawyer include the duties of competence and confidentiality. Model Rule 5.3: Responsibilities Regarding Nonlawyer Assistants was amended in 2012 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 ensure that nonlawyers, both inside and outside a law firm, provide services in compliance with an attorney's ethical duties, including confidentiality.

Ethics Opinions. A number of state ethics opinions, for over a decade, have addressed professional responsibility issues related to security in attorneys' use of various technologies. Consistent with the Ethics 20/20 amendments, they generally require competent and reasonable safeguards.

Examples include State Bar of Arizona, Opinion No. 05-04 (July 2005), 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); State Bar of California, Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2010-179; and New York State Bar

Association Ethics Opinion 1019, “Confidentiality; Remote Access to Firm’s Electronic Files,” (August, 2014).

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. Depending on the circumstances, an attorney may be required to avoid using a particular technology or to advise a client of the risks and seek informed consent if appropriate safeguards cannot be employed.

There are now multiple ethics opinions on attorneys’ use of cloud computing services like online file storage and software as a service (SaaS).[iii] 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 recent opinion on safeguarding client data is ABA Formal Opinion 477, “Securing Communication of Protected Client Information” (May 2017). While focusing on electronic communications, it also explores the general duties to safeguard information relating to clients in light of current threats and the Ethics 20/20 technology amendments to the Model Rules. Its conclusion includes:

Rule 1.1 requires a lawyer to provide competent representation to a client. Comment [8] to Rule 1.1 advises lawyers that to maintain the requisite knowledge and skill for competent representation, a lawyer should keep abreast of the benefits and risks associated with relevant

technology. Rule 1.6(c) requires a lawyer to make "reasonable efforts" to prevent the inadvertent or unauthorized disclosure of or access to information relating to the representation.

Most recently, the ABA issued Formal Opinion 483, "Lawyers' Obligations After an Electronic Data Breach or Cyberattack" (October 17, 2018). The opinion reviews lawyers' duties of competence, confidentiality and supervision in safeguarding confidential data and in responding to data breaches. It discusses the obligations to monitor for a data breach, stopping a breach and restoring systems, and determining what occurred. It finds that Model Rule 1.15: Safeguarding Property applies to electronic client files as well as paper client files and requires the care required of a professional fiduciary.

The opinion concludes:

> Even lawyers who, (i) under Model Rule 1.6(c), make "reasonable efforts to prevent the unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," (ii) under Model Rule 1.1, stay abreast of changes in technology, and (iii) under Model Rules 5.1 and 5.3, properly supervise other lawyers and third-party electronic-information storage vendors, may suffer a data breach. When they do, they have a duty to notify clients of the data breach under Model Rule 1.4 in sufficient detail to keep clients "reasonably informed" and with an explanation "to the extent necessary to permit the client to make informed decisions regarding the representation."

The key professional responsibility requirements from these various opinions on attorneys' use of technology are competent and reasonable measures to safeguard client data, including an understanding of limitations in attorneys' knowledge, obtaining appropriate assistance, continuing security awareness, appropriate supervision, and ongoing review as technology, threats, and available safeguards evolve. They also require obtaining clients' informed consent, in some circumstances, and notifying clients of a breach or compromise. It is important for attorneys to consult the rules, comments, and ethics opinions in the relevant jurisdiction(s).

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 to confidentiality. It is important for attorneys to understand and address these risks.

The Ethics 2000 revisions to the Model Rules, over 15 years ago, added Comment [17] (now 19]) to Model Rule 1.6. For electronic communications, it requires "reasonable precautions to prevent the information from coming into the hands of unintended recipients." It provides:

…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…

This Comment requires attorneys to take "reasonable precautions" to protect the confidentiality of electronic communications. Its language about "special security measures" has often been viewed by attorneys as providing that they 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 qualification - "if the method of communication affords a reasonable expectation of privacy."

There are, however, questions about whether unencrypted Internet e-mail affords a reasonable expectation of privacy. Respected security professionals for years have compared the security of unencrypted e-mail to postcards or postcards written in pencil.[iv] A June 2014 post by Google on the *Google Official Blog*[v] and a July 2014 *New York Times*

"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."
Google

article[vi] use the same analogy – comparing the security of unencrypted e-mails to postcards and comparing encryption to envelopes.

Comment [19] to Rule 1.6 also lists "the extent to which the privacy of the communication is protected by law" as a factor to be considered. The federal Electronic Communications Privacy Act[vii] and similar state laws make unauthorized interception of electronic communications a crime. Some observers have expressed the view that this should be determinative and attorneys should not be required to use encryption. The better view is to treat legal protection as only one of the factors to be considered. As discussed below, some of the newer ethics opinions conclude that encryption may be a reasonable measure that should be used, particularly for highly sensitive information.

Ethics Opinions – Electronic Communications. An ABA ethics opinion in 1999 and several state ethics opinions concluded that special security measures, like encryption, are not generally required for confidential attorney e-mail.[viii] However, these opinions, like Comment [19], contain qualifications that limit their general conclusions.

Consistent with the questions raised by security experts about the security of unencrypted e-mail, some ethics opinions express a stronger view that encryption may sometimes 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."[ix] This was over ten years ago.

California Formal Opinion No. 2010-179, Pennsylvania Formal Opinion 2011-200 and Texas Ethics Opinion 648 (2015) provide that encryption may sometimes be required. A July, 2015 ABA article notes **"**The potential for unauthorized receipt of electronic data has caused some experts to revisit the topic and issue [ethics] opinions suggesting that in some circumstances, encryption or other safeguards for certain email communications may be required."[x]

"...[P]articularly strong protective measures, like encryption, are warranted in some circumstances."

On May 11 of 2017, the ABA Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 477, "Securing Communication of Protected Client Information." The Opinion revisits attorneys' duty to use encryption and other safeguards to protect e-mail and electronic communications in light of evolving threats, developing technology, and available safeguards. It suggests a fact-based analysis and concludes "the use of unencrypted routine email generally remains an acceptable method of lawyer-client communication," but "particularly strong protective measures, like encryption, are warranted in some circumstances."

Opinion 477, consistent with these newer opinions and the article, concludes:

A lawyer generally may transmit information relating to the representation of a client over the Internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, **a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.** (Emphasis added.)

The Opinion references the Ethics 20/20 amendments to Comment [18] to Model Rule 1.6 and its discussion of factors to be considered in determining reasonable and competent efforts. It provides general guidance and leaves details of their application to attorneys and law firms, based on a fact-based analysis on a case-by-case basis.

In addition to complying with any applicable ethics and legal requirements, the most prudent approach to the ethical duty of protecting electronic communications is to have an express understanding with clients (preferably in an engagement letter or other writing) 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 where all attorneys should have encryption available for use in appropriate circumstances.

Common Law and Contractual Duties. Along with the ethical duties, there are 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, including 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 increasing instances when lawyers have contractual duties to protect client data, particularly for clients in regulated industries, such as health care and financial services that have regulatory requirements to protect privacy and security.

For example, the Association of Corporate Counsel has adopted *Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information* that companies can use for security requirements for outside counsel.[xi]

Regulatory Duties. Attorneys and law firms that have specified personal information about their employees, clients, clients' employees or customers, opposing parties and their employees, or even witnesses may also be covered by federal and state laws that variously require reasonable safeguards for covered information and notice in the event of a data breach.[xii]

II. Complying with the Duties

Understanding all of the applicable duties is the first step, before moving to the challenges of compliance by designing, implementing and maintaining an appropriate risk-based information security program. It should address people, policies and procedures, and technology and be appropriately scaled to the size of the practice and the sensitivity of the information.

Information Security Overview. 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."[xiii] 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 Information Technology department or consultants. While IT has a critical role, everyone, including management, all attorneys, and all support personnel, must be involved for effective security.

The best technical security is likely to fail without adequate attention to people and policies and procedures.

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 an ABA report aptly put it:[xiv]

> 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.)

Information security is best viewed as a part of the information governance process. Information governance manages documents and data from creation to final disposition – including security and privacy.[xv]

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

> **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.

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

The first step for a security program is assigning responsibility for security. This includes defining who is in charge of security and defining everyone's role, including management, attorneys and support personnel.

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

An information security program should cover the core security functions: **identify, protect, detect, respond and recover.** While detection, response, and recovery have always been important parts of security, they have too often taken a back seat to protection. Since security incidents and data breaches are increasingly viewed as sometimes being inevitable, these other functions have taken on increased importance. Gartner, a leading technology consulting firm, has predicted that by 2020, 60% of enterprises' information security budgets will be allocated for rapid detection and response approaches, up from less than 10% in 2014.[xvii]

The requirement for lawyers is reasonable security, not absolute security. For example, 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 Model 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. 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.

The Ethics 20/20 amendments to Comment 18 to Rule 1.6 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).

This is a risk-based approach that is now standard in information security.

A comprehensive security program should be based on a standard or framework. Examples include the National Institute for Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, (April 2018), other more comprehensive NIST standards, like NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013) and standards referenced in it (a comprehensive catalog of controls and a process for selection and implementation of them through a risk management process) (designed for government agencies and large organizations), and the International Organization for Standardization's (ISO), ISO/IEC 27000 family of standards, (consensus international standards for comprehensive Information Security Management Systems (ISMS) and elements of them). (See NIST and ISO references in Additional Information below for references to these standards and frameworks.)

These standards can be a challenge for small and mid-size firms. In October of 2018, the Federal Trade Commission launched a new website, Cybersecurity for Small Business, which includes links to a number of security resources that are tailored to small businesses.[xviii] It is a joint project of the FTC, NIST, the U.S. Small Business Administration, and the U.S. Department of Homeland Security. NIST's *Small Business Information Security: The Fundamentals, NISTR 7621, Revision 1* (November 2016) provides NIST's recommendations for small businesses based on the *Framework*.[xix] In March of 2019, NIST launched its Small Business Cybersecurity Corner website.[xx]

A comprehensive information security program should include:

- **Assignment of responsibility for security,**
- **An inventory of information assets and data,**
- **A risk assessment,**
- **Appropriate administrative, technical and physical safeguards to address identified risks,**
- **Managing new hires, current employees and departing employees**
- **Training,**
- **An incident response plan,**
- **A backup and disaster recovery program,**
- **Managing third-party security risks, and**
- **Periodic review and updating.**

Attorneys and law firms will often need assistance in developing, implementing, and maintaining information security programs because they do not have the requisite knowledge and experience. For those who need assistance, it is important to find an IT consultant with knowledge and experience in security or a qualified security consultant. Qualified consultants can provide valuable assistance in this process. An increasing number of law firms are using service providers for assistance with developing and implementing security programs, for third-party review of security, and for services like security scans and penetration testing to identify vulnerabilities. A growing trend is to outsource **part** of the security function by using a managed security service provider for functions such as remote administration of security devices like firewalls, remote updating of security software, and 24 X 7 X 365 remote monitoring of network security.

Cyber Insurance. Law firms are increasingly obtaining cyber insurance to transfer some of the risks to confidentiality, integrity, and availability of data in their computers and information systems. This emerging form of insurance can cover gaps in more traditional forms of insurance, covering areas like restoration of data, incident response costs, and liability for data breaches. Because cyber insurance is an emerging area of coverage and policies differ, it is critical to understand what is and is not covered by policies and how they fit with other insurance. The ABA Center for Professional Responsibility has published *Protecting Against Cyber Threats: A Lawyer's Guide to Choosing a Cyber-Liability Insurance Policy* that provides guidance in this area.[xxi]

III. Conclusion

Attorneys have ethical and common law duties to take competent and reasonable measures to safeguard information relating to clients and often have contractual and regulatory duties. These duties provide 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. The safeguards should be included in a risk-based, comprehensive security program. Attorneys have three options for complying with these duties: know the requirements, threats and relevant safeguards, learn them, or get qualified assistance. For most attorneys, it will be a combination of all three.

IV. Additional Information

Note: The American Bar Association website is going through a major revamping. Some of the links below and in the endnotes may change.

American Bar Association, Business Law Section, Cyberspace Law Committee, http://apps.americanbar.org/dch/committee.cfm?com=CL320000

American Bar Association, Cybersecurity Resources, www.americanbar.org/groups/leadership/office_of_the_president-old/cybersecurity/resources.html, provides links to cybersecurity materials and publications by various ABA sections, divisions and committees

American Bar Association, Cybersecurity Legal Task Force www.americanbar.org/groups/leadership/office_of_the_president/cybersecurity.html

American Bar Association, Law Practice Division, www.lawpractice.org, including the Legal Technology Resource Center www.americanbar.org/groups/departments_offices/legal_technology_resources.html

American Bar Association, *A Playbook for Cyber Events, Second Edition* (American Bar Association 2014)

American Bar Association, Section of Litigation, Privacy and Data Security Committee, www.americanbar.org/groups/litigation/committees/privacy-data-security/about.

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

John T. Bandler, *Cybersecurity for the Home and Office: The Lawyer's Guide to Taking Charge of Your Own Information Security* (American Bar Association 2017)

Center for Internet Security, a leading security organization that publishes consensus-based best security practices like the *CIS Controls* and *Secure Configuration Benchmarks*, www.cisecurity.org

Daniel Garrie and Bill Spernow, *Law Firm Cybersecurity* (American Bar Association 2017)

Federal Trade Commission (FTC), Data Security Resources for Business, www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security, Small Business Cybersecurity, www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity

ILTA (International Legal Technology Association) LegalSEC, , provides the legal community with guidelines for risk-based information security programs, including publications, the LegalSEC security initiative, peer group discussions, webinars, an annual LegalSEC Summit conference and other live programs; some materials are publicly available while others are available only to members, http://connect.iltanet.org/resources/legalsec?ssopc=1

International Organization for Standardization (ISO), publishes the ISO/IEC 27000 family of standards, consensus international standards for comprehensive Information Security Management Systems (ISMS) and elements of them, www.iso.org/isoiec-27001-information-security.html

National Institute of Standards and Technology (NIST), http://csrc.nist.gov/publications, publishes numerous standards and publications, including the *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1,* (April 2018) and *Small Business Information Security: The Fundamentals, NISTR 7621, Revision 1* (November 2016) and Small Business Cybersecurity Corner website, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf and www.nist.gov/itl/smallbusinesscyber

SANS Institute, www.sans.org, a leading information research, education, and certification provider, includes resources like the *SANS Reading Room*, the *Critical Security Controls*, *Securing the Human*, and OUCH! (a monthly security newsletter for end users)

Sharon D. Nelson, David G. Ries and John W. Simek, *Encryption Made Simple for Lawyers* (American Bar Association 2015)

Sharon D. Nelson, David G. Ries and John W. Simek, *Locked Down: Practical Information Security for Lawyers, Second Edition* (American Bar Association 2016)

Jill D. Rhodes and Robert S. Litt, *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals, Second Edition* (American Bar Association 2017)

The Sedona Conference, *Commentary on Privacy and Information Security: Principles and Guidelines for Lawyers, Law Firms, and Other Legal Service Providers* (November 2015)

US-CERT, part of the U.S. Department of Homeland Security, www.us-cert.gov,

includes resources for implementing the NIST Framework (businesses www.us-cert.gov/ccubedvp/getting-started-business) and (small and midsize businesses www.us-cert.gov/ccubedvp/getting-started-smb)

David G. Ries is of counsel in the Pittsburgh, PA office of Clark Hill PLC, where he practices in the areas of environmental, technology, and data protection law and litigation. For over 20 years, he has increasingly focused on cybersecurity, privacy, and information governance. He has used computers in his practice since the early 1980s and since then has strongly encouraged attorneys to embrace technology – in appropriate and secure ways.

Dave frequently speaks and writes nationally on legal ethics, technology, and technology law topics. He is a coauthor of *Locked Down: Practical Information Security for Lawyers, Second Ed.* (ABA 2016) and *Encryption Made Simple for Lawyers (ABA 2015)* and a contributing author to *Information Security and Privacy: A Legal, Business and Technical Handbook, Second Edition* (American Bar Association 2011). He served on the ABA TECHSHOW Planning Board from 2005 through 2008 and is a member of the ABA Cybersecurity Legal Task Force, InfraGard's Legal Industry Special Interest Group, and ILTA's LegalSEC.

---

[i] FBI Director, RSA Cybersecurity Conference (March 1, 2012) https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

[ii] ABA Model Rulers of Professional Conduct (2018) (Model Rules).

[iii]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).

[iv] E.g., Bruce Schneier, *E-Mail Security - How to Keep Your Electronic Messages Private,* (John Wiley & Sons, Inc. 1995) p. 3, Bruce Schneier, *Secrets & Lies: Digital Security in a Networked Work*, (John Wiley & Sons, Inc. 2000) p. 200, and Larry Rogers, *Email – A Postcard Written in Pencil*, Special Report, (Software Engineering Institute, Carnegie Mellon University 2001).

[v] "Transparency Report: Protecting Emails as They Travel Across the Web," *Google Official Blog* (June 3, 2014) http://googleblog.blogspot.com/2014/06/transparency-report-protecting-emails.html.

[vi] Molly Wood, "Easier Ways to Protect Email from Unwanted Prying Eyes," *New York Times* (July 16, 2014) www.nytimes.com/2014/07/17/technology/personaltech/ways-to-protect-your-email-after-you-send-it.html?_r=0.

[vii] 18 U.S.C. §§ 2510-2522.

[viii] For example, 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.").

[ix] 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."

[x] Peter Geraghty and Susan Michmerhuizen, "Encryption Conniption," *Eye on Ethics, Your ABA* (July 2015) (www.americanbar.org/publications/youraba/2015/july-2015/encryption-conniption.html).

[xi] www.acc.com/advocacy/upload/Model-Information-Protection-and-Security-Controls-for-Outside-Counsel-Jan2017.pdf.

[xii] For example, Internal Revenue Code, 26 U.S.C Section 6713, Internal Revenue Procedure 2007-40, Gramm-Leach-Bliley Act, 15. U.S.C. Sections 6801-6809 and National Conference of State Legislatures - State Data Security Laws (www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx) and State Security Breach Notification Laws (www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx).

[xiii] Bruce Schneier, *Secrets and Lies - Digital Security in a Networked World* (John Wiley & Sons, Inc. 2000) at p. xii.

[xiv] Joshua Poje, "Security Snapshot: Threats and Opportunities," ABA TECHREPORT 2013 (ABA Legal Technology Resource Center 2013).

[xv] See the Information Governance Reference Model, published by EDRM, an organization operated by Duke Law School that publishes resources for e-discovery and information governance. www.edrm.net/frameworks-and-standards/information-governance-reference-model.

[xvi] Available at www.americanbar.org/content/dam/aba/images/abanews/2014am_hodres/109.pdf.

[xvii] http://blogs.gartner.com/anton-chuvakin/2014/02/24/new-research-on-dealing-with-advanced-threats.

[xviii] www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity.

[xix] https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf.

[xx] www.nist.gov/itl/smallbusinesscyber.

[xxi] Eileen R. Garczynski, *Protecting Against Cyber Threats: A Lawyer's Guide to Choosing a Cyber-Liability Insurance Policy* (American Bar Association 2016) and Eileen R. Garczynski, "Protecting Firm Assets with Cyber Liability Insurance," *Business Law Today* (September 2016), www.americanbar.org/publications/blt/2016/09/05_garczynski.html

Disasters and Data Breaches: The ABA Speaks

by Sharon D. Nelson, Esq. and John W. Simek

DID THE PARADE PASS YOU BY?

In 2018, the ABA released two very significant ethical opinions. One was Formal Opinion 483: Lawyers' Obligations After an Electronic Data Breach or Cyberattack (October 17, 2018). The other was Formal Opinion 482: Ethical Obligations Related to Disasters (September 19, 2018).

To our surprise, we rarely find CLE attendees who are aware of these opinions. Even those who are aware of them do not seem to know their details or understand their implications. Hence the inspiration for this article. Both opinions should be carefully read by lawyers seeking to understand their ethical duties in the event of a disaster (natural or man-made) or a data breach (which is of course a very specific form of a disaster)!

DATA BREACHES AND HEADLESS CHICKEN MODE

In our line of work, we see a lot of law firms who have been breached. "Headless Chicken Mode" is our name for the reaction of those who have not prepared for a breach – they have no incident response plan. They run in circles, hysterical, with no idea what to do. Sadly, there are a lot of law firms without an incident response plan –a 2018 study by IBM Resilient and the Ponemon Institute revealed that half of all organizations described their incident response plans as informal, ad hoc, or completely non-existent.

Today, for law firms, not having a formal incident response plan is inexcusable – and unethical under these new opinions. With respect to cyberattacks, our own experience has shown:

- The faster you catch a cyberattack, the less it will cost you and the faster you can recover.
- You are no stronger than your weakest link (usually your employees).
- With a good incident response plan, preparation is 2/3 of the effort, and the remaining 1/3 is solving the problems when an attack occurs.

THE CLOUD IS YOUR FRIEND

Whether you have a data breach or another form of disaster, the cloud is your friend. Opinion 482 talks about the duty of communication required by Rule 1.4, which requires lawyers to communicate regularly with clients and keep their clients reasonably apprised about their cases. Following a disaster, a lawyer must evaluate available methods to maintain communication with clients. The opinion instructs that lawyers should keep electronic lists of current clients in a manner that is "easily accessible."

The opinion also references Rule 1.1, which requires lawyers to consider the benefits and risks of relevant technology. It also notes that lawyers "must evaluate in advance storing files electronically" such they can access them after a disaster.

If your office is flooded (and maybe your home where you leave your backups), the best way to access client contact information is via the cloud. More and more, ABA opinions are not so gently pushing law firms toward the cloud. We agree completely that essential law firm data should, at the very least, be backed up in the cloud. Keep your data on premise if you like with an on premise backup, but make sure there is a copy in the cloud. Today, that is just a common sense precaution and almost universally accepted by legal technologists.

Yes, you need a reputable cloud provider, and you need to read the Terms of Service and ask questions regarding the security of client data, but there are many acceptable and respected cloud providers available to lawyers today – the fear of the cloud has faded. In fact, law firms tend to fear NOT being in the cloud.

SAFEGUARDING CLIENT PROPERTY

There was a time – and not so long ago – where lawyers obeyed Rule 1.15 (safeguarding client property) by locking up paper files. It is a whole new world today. If client data is destroyed, the opinion says lawyers can attempt to reconstruct files by obtaining documents from other sources. If they cannot, they must notify the clients of the loss of the files. To prevent such losses, "lawyers should maintain an electronic copy of important documents in an off-site location that is updated regularly." Yup, we're back to the cloud again.

In many law firms, cloud backups are updated as frequently as every 15 minutes. While that may not be ethically required, most firms at least perform daily cloud backups.

MONEY, ATTORNEY WITHDRAWAL AND GREED

As we saw with Katrina in particular, disasters can impact financial institutions and, therefore, client funds. Thus, the opinion says that lawyers "must take reasonable steps in the event of a disaster to ensure access for funds the lawyer is holding in trust." This largely presupposes that you are doing electronic banking, which most firms are, and can therefore access client funds once you have an internet connection (which means you need a redundant internet connection). You may also need to have another trusted signatory or, if the worst happens, have a successor lawyer to wind up your practice. Gloomy thoughts, but it's like having a will – simply a necessity of life and your profession.

In a true disaster, you may not be able to perform legal services and may have to withdraw. Under Rule 1.16, "In determining whether withdrawal is required, lawyers must assess whether the client needs immediate legal services that the lawyer will be unable to timely provide." Again, we harken back to Katrina, where many lawyers were forced by circumstances to withdraw from representation. Needless to say, you must seek the court's permission to withdraw as required by law and court rules. A good practice tip is to address in your engagement letter how to contact you in the event of a disaster.

When the U.S. Virgin Islands firm Bolt Nagi lost its St. Thomas office during Irma and Maria, our friend and colleague Tom Bolt had the law firm website temporarily altered to display his cell phone number. Tom, the firm's managing partner, certainly went the extra mile to make sure firm clients could contact him.

Many people seek to gain from disaster victims. The opinion warns lawyers that they should not take advantage of disaster victims for personal gain. "Of particular concern is the possibility of improper solicitation in the wake of a disaster." While the warning is well taken, the authors note anecdotally that they were never prouder of the legal profession than after Katrina, when so many lawyers and legal professionals reached out to help lawyers (and their clients) impacted by the flood waters of Katrina.

PRACTICING IN OTHER STATES

On this issue, you should read the opinion itself carefully. If you are displaced from your jurisdiction and seek to practice elsewhere temporarily, in accordance with Rule 5.5(c), you must obtain approval from the new jurisdiction.

The opinion cites a key provision of the ABA Model Court Rule on Provision of Legal Services Following Determination of Major Disaster. That rule provides in part that a lawyer displaced by a disaster "may provide legal services in this jurisdiction on a temporary basis if permitted by order of the highest court of the other jurisdiction."

Many lawyers simply want to volunteer to help disaster victims. The opinion states that, "Out-of-state lawyers may provide representation to disaster victims in the affected jurisdiction only when permitted by that jurisdiction's laws or rules, or by order of the jurisdiction's highest court."

The ABA Model Court Rule on Provision of Legal Services Following Determination of Major Disaster requires that "the supreme court of the affected jurisdiction must declare a major disaster and issue an order that allows lawyers in good standing from another jurisdiction to temporarily provide pro bono legal services in the affected jurisdiction through a nonprofit bar association, pro bono program, legal services program or other organization designated by the courts."

Just make sure you follow the rules. It is also helpful to volunteer your time through the ABA or other pro bono services providers. A good many of our ABA colleagues went down to New Orleans to help lawyers reestablish their practices. Even from Virginia, we took five Tulane Law School students under our wings and purchased/configured new laptops for them, which they took to Georgetown, which generously allowed them to continue their legal education there.

There is always a way to help without getting yourself in ethical trouble!

THE MOST LIKELY DISASTER: A DATA BREACH

The Cyber Readiness Report 2019, commissioned by global insurer Hiscox, found that 61% of global firms have been breached in the past year. While not specific to law firms, that is a dramatic increase – and law firms are by no means immune. It fact, we are a target-rich environment because we hold the data of so many

clients. And, to be frank, law firm security remains weak, especially in solo/small/midsized firms.

Data breaches are silent and deadly – not at all like the disasters recounted above. If you want to feel your blood pressure rise, Google “FireEye Live Cyber Threat Map” and watch the attacks in real time. In the last several years, we have witnessed cyberattacks routinely conducted by bots and seen attacks powered by artificial intelligence.

THE ABA SPEAKS TWICE IN TWO YEARS ON CYBERSECURITY

The ABA’s Formal Opinion 483, "Lawyers' Obligations After an Electronic Data Breach or Cyberattack" builds on the Standing Committee on Ethics and Professional Responsibility’s Formal Opinion 477R released in May 2017, which set forth a lawyer's ethical obligation to secure protected client information when communicating digitally.

The new opinion states: "When a breach of protected client information is either suspected or detected, Rule 1.1 requires that the lawyer act reasonably and promptly to stop the breach and mitigate damage resulting from the breach."

The opinion discusses Model Rule 1.1 (competence), Model Rule 1.4 (communications), Model Rule 1.6 (confidentiality of information), Model Rule 1.15 (safekeeping property), Model Rule 5.1 (responsibilities of a partner or supervisory lawyer) and Model Rule 5.3 (responsibilities regarding nonlawyer assistance). Where we have gone through these rules with respect to Opinion 482, we will not repeat ourselves here unless there are additional aspects to cover.

There is a "rule of reason" overtone to the opinion, which states, "As a matter of preparation and best practices, however, lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach. . . The decision whether to adopt a plan, the content of any plan and actions taken to train and prepare for implementation of the plan should be made before a lawyer is swept up in an actual breach."

Wait – didn’t we say that earlier in the article? In fairness, this is what all cybersecurity experts have said for a very long time – and, in our experience, all large firms tend to have an incident response plan. The smaller firms? Not so

much. No one is saying that a law firm need to be invincible because that is not possible. As the opinion states, "the potential for an ethical violation occurs when a lawyer does not undertake reasonable efforts to avoid data loss or to detect cyber-intrusion, and that lack of reasonable effort is the cause of the breach." There you have it in a nutshell.

ZOMBIE DATA

Is there anything not somehow affiliated with Zombies these days? For those of you not familiar with the term, zombie data is also known as "dark data," – data you don't know you have until after you have a data breach. The opinion takes a "throw out the trash approach" and recommends, in a footnote, that firms should have data retention policies that limit their possession of personally identifiable information. What you don't have can't hurt you.

As an aside, zombie data pops up all the time in e-discovery and causes a huge amount of expense, not to mention the negative effects it can have on a case when it is suddenly discovered. If you don't need it, and are not legally required to preserve it, get rid of it!

COMMUNICATING DATA BREACHES WITH CLIENTS

Since data breaches cannot entirely be avoided, the opinion says, "When a lawyer knows or reasonably should know a data breach has occurred, the lawyer must evaluate notice obligations. Model Rule 1.4. Rule 1.4(a)(3) provides that a lawyer must "keep the client reasonably informed about the status of the matter." Rule 1.4(b) provides: "A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation."

First, law firms must halt the attack, mitigate the damage and then make reasonable efforts to assess the data that may have been exposed. Not so easy. You can contract ransomware which exfiltrates your data before encrypting your files (therefore a data breach) or ransomware which only encrypts your files and then asks a ransom for the decryption key (therefore not a data breach). The opinion notes that your efforts in determining what happened and fixing it may be through qualified experts.

If you need to report an incident to a government agency, you are still bound by Rule 1.6. We sense there may be some tension over trying to report and trying to

maintain client confidential data. How do you know if the disclosure is "impliedly authorized?" Read the opinion fully to understand all the nuances of this dilemma.

Under Rule 1.4, the opinion says bluntly that you must inform a current client of a data breach that impacts their material confidential information. Forgive us for how we say this, but this duty is often honored "in the breach." Typically, law firms say they have no evidence that the confidential information was accessed or used. It's often a rusty nail, but that's where they frequently hang their hat.

What exactly are you supposed to tell clients in your disclosure? The opinion is a little vague, saying that "the disclosure must be sufficient to provide enough information for the client to make an informed decision as to what to do next, if anything."

The opinion dodges a bit when it comes to former clients, finding no duty to notify former clients unless there is something mandating notification.

FINAL WORDS

These are good opinions, worthy of a careful read. As is now customary with all opinions dealing with technology, modification of these opinions may need to be made over time. The two opinions are good roadmaps – and we hope many law firms who are woefully unprepared for disasters, including data breaches, use them as intended to prepare for the worst before it happens.

Sharon D. Nelson, Esq. is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She a co-author of 17 books published by the ABA. snelson@senseient.com.

John W. Simek is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm. jsimek@senseient.com.

A Roadmap for Lawyers With Cybersecurity Paralysis

by Sharon D. Nelson, Esq. and John W. Simek

We understand why lawyers have cybersecurity paralysis. They don't understand cybersecurity, experts disagree on the best steps to take, the majority of cybersecurity measures involve spending time and money – and to top it off, the threats and defenses against those threats change daily. Here's a brief roadmap to where you should be going.

By the Numbers: Where We Stand Today

Thanks to the ABA's 2018 Legal Technology Survey Report, we have some solid numbers to ponder as we construct our roadmap. Looking strictly at the big picture statistics, these were the ones we found most significant.

- 23% of respondents reported that their firm had been breached at some point.
- Of those reporting that they had been breached, the percentage breached generally increased with firm size until you got to large firms - 14% were solos, 24% for firms with 2-9 and 20-49 attorneys, 42% with 50-99 attorneys, and 31% with 100+ attorneys.
- 60% reported that their firms had not experienced a data breach. It is important to note that it is extremely possible that many firms experienced a breach and never detected it.
- 9% of those breached notified clients and 14% notified law enforcement.
- Of those breached, 41% reported downtime/loss of billable hours, 40% reported consulting fees for remediation of the problems, 11% reported loss or destruction of files, and 27% reported replacement of hardware/software.
- 40% reported experiencing an infection with viruses/malware/spyware, with the greater number occurring in firms with 2-49 attorneys and the lowest in firms with 500+ attorneys.
- 34% reported having cyberinsurance coverage (the percentage is growing, but slowly).
- 24% reported using full-drive encryption, a low number in these days.
- 29% reported using encryption of email for confidential/privileged data sent to clients.

Without bombarding you with numbers, the smaller the firm, the less likely it was to have a policy covering document retention, acceptable computer use, remote access, social media, personal technology use and employee privacy.

Perhaps most startling to us was the fact that only 25% reported having an incident response plan, a critical cybersecurity component. Larger firms were more likely to have such a plan. In general, larger firms have a bigger attack surface, but they also have more resources to devote to cybersecurity. We will focus in this article on solo/small/mid-size firms as we try to lay out a roadmap to cybersecurity.

Security Assessments Are Essential

You can't fix what you don't know is broken. That's a fact. We are now at a point in time where 11% of attorneys have received from a client or prospective client a request for a security assessment. 34% have received some sort of client security requirements document. While the survey didn't ask about assessments required by insurance companies in order to get cyberinsurance, we know from our own clients that these are becoming more prevalent.

Even if no one requires you to do an assessment, you absolutely need one – and it should be done at least annually. Why don't firms have an assessment done? Mostly because lawyers fear the costs of the assessments – and the costs they may incur in fixing what's wrong.

So let us try to allay some fears. While it's true that large law firms will generally seek out large (and therefore expensive) cybersecurity firms, it is equally true that there are many smaller cybersecurity firms with reasonable fixed-fee prices for doing an assessment and giving you a report identifying your vulnerabilities.

What should you be looking for besides a reasonable price? References from colleagues (who have no dog in the hunt) are useful. Make sure the company has true cybersecurity certifications. IT certifications are not cybersecurity certifications. Also make sure the report will follow the guidelines of a reputable organization such as the Center for Internet Security.

What you want as an end result is to know what critical vulnerabilities you have so those can be fixed right away. After that, the report will identify medium and low risks. Address medium risks as soon as you can. The idea is to plan a timeline, often constructed around budget constraints or impact on productivity. The low risks should of course be addressed, but they don't carry the level of concern that critical and medium risks do.

Train Your Employees!

Your most valuable asset (your employees) are also a great threat. They are often moving too fast and easily duped by phishing emails. Phishing emails often and successfully target law firm. Perform phishing simulations where employees receive carefully constructed emails specific to your firm. If they do not see the red flags and click on a link or attachment (or answer an email leading to a follow-up conversation asking for monies, gift cards etc.), you will see how much training – and retraining - is needed.

Training should be annual, mandatory and without mobile devices present. The partners should be there, leading by example. Believe it or not, training is not very expensive – again, stick with smaller companies with cybersecurity certifications. Don't use your in-house folks – they simply don't carry a big enough stick – outsiders are invariably a better solution. Again, it's a good idea to get referrals from colleagues. You want trainers who can both educate and entertain. If they cannot keep the attention of your employees, you are probably throwing money down a rat hole.

Happily, we are seeing more and more firms of all sizes investing in training. It might surprise you, but the employees generally enjoy the training and feel more confident in their ability to spot phishing emails, recognize social engineering attacks, etc. This is an excellent way of creating a culture of cybersecurity.

The Power of Policies

Policies in law firms tend to be static. There is a big push to get some policies in place and then nothing happens – sometimes for years. But policies are invaluable in all sorts of ways. They set the expectations of your employees. If employees disobey them, they will expect consequences, up to and including termination, depending on the severity of the violation.

As the world invariably changes (think of the policies that sufficed twenty years ago!), all policies should be reviewed yearly and revised as needed. Train employees on them every year – they will invariably forget portions of policies that are very important.

Many policies involve cybersecurity but they have different names, which can be confusing. The most common, by whatever name, are:

- Acceptable use policy
- Social media policy
- Remote access policy
- BYOD (Bring Your Own Device) policies
- Access control policies (passwords, multifactor authentication, biometric authentication, etc.)
- Backup policy
- Vendor access policy
- Retention and destruction of data policy (let us interject here that minimizing the data you retain is free – and greatly reduces your risk)
- Disaster recovery policy
- Encryption policy
- Reporting lost or stolen device policy
- Employee privacy (which may mean the absence of privacy on your network)

The Critical Incident Response Plan

If you don't have an incident response plan and you then suffer a breach, you will invariably be running around in headless chicken mode. We have borne witness to this reaction many times – you don't want to be in that mode.

The way to avoid it is to have a good incident response. The elements of such a plan are not all that complicated. Here are the essentials:

- Contact information for your regional FBI office
- Contact information for a data breach lawyer

- Contact information for the attorney who will oversee the breach response and any others in the firm who may be involved
- Contact information for a digital forensic company (to investigate and remediate the breach)
- Contact information for your insurance company (you may be required to report a breach/incident in a given period of time or lose benefits)
- Contact information for your bank (in case you need to warn them to be wary of suspicious transactions - banks are accustomed to this)
- Contact information for a public relations firm (small firms are less likely to use these services)
- Who needs to be informed? Clients? Vendors? The state attorney general? Make sure to have a copy of your state's data breach notification law kept with the plan.
- Plans for preservation of information to assist in the breach investigation such as gathering all logged data and taking impacted devices off-line
- Steps to resume operation

You should do annual reviews of the plan, including (at least) tabletop exercises where you go through various scenarios, adding and subtracting issues and problems (managing partner is climbing a mountain in Asia and inaccessible, the electric grid is down, etc.).

The Right Technology at the Right Price

So . . . you're not a mega law firm and you are budget conscious. No worries, it's a big club. So here is our basic technology advice with this stern warning: No technology is invincible.

Let's start with some simple and free advice. Make sure you apply all patches and updates as they become available. Failure to patch leaves you vulnerable to a security incident. Trust us, the bad guys are constantly scouring the Internet looking for those that are vulnerable to a known hack.

Obviously, you need some sort of endpoint protection. This means there should be some sort of security software installed on all your computers, servers and mobile devices. In the old days it was called anti-virus software, but today's endpoint protection is really a security suite that contains such things as a firewall, anti-malware protection, anti-virus, encryption, etc. Endpoint protection is a good start, but you really need some vision into events happening at the endpoints. According to a report by Sophos and market research company Vanson Bourne, one in five IT managers didn't know how an attacker got in, even after discovering the threat. This has given rise to Endpoint Detection and Response (EDR) tools to provide vision into security events.

Another important concern is edge protection. This is where you would install some sort of firewall appliance. One of our favorite products (no we don't get any commissions) is the Meraki product line by Cisco. The Meraki is a combination firewall, intrusion detection system (IDS), intrusion prevention system (IPS) and wireless access point (AP). The device itself is only a

few hundred dollars and the annual subscription for the software is only a few hundred dollars as well. Best of all, the subscription includes continuing updates to your protection as new threats are discovered – and they happen automatically – you don't have do a thing or spend another dime. You may recognize the combined functions from the old days of unified threat management (UTM) devices. You don't see the UTM term used these days, but effectively that's what devices like Meraki are.

Another area to focus on is mobile device management (MDM). It is no secret that we are a mobile society and our smartphones are really powerful computers that can also make phone calls. Larger firms will invest in MDM solutions such as Airwatch, Mobileiron or Microsoft's Intune. We would suggest that the solo and small firm lawyer look to the built-in controls contained in Active Sync. If you have your own Exchange server or use Exchange Online with Office 365, Active Sync is a free feature that can enforce device encryption, enforce lock codes and even remotely wipe the device.

Final Thoughts

As we write this the week after coming back from speaking at ABA TECHSHOW®, we are reminded that much of the cybersecurity advice above was echoed there. One of our favorite slides had the words "Store Less. Delete More." That might have been the best, most succinct advice we heard during the conference. Words to live by!

Sharon D. Nelson, Esq. is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She a co-author of 17 books published by the ABA. snelson@senseient.com.

John W. Simek is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm. jsimek@senseient.com.

A Baker's Dozen: Thirteen Cybersecurity Questions Lawyers Ask

by Sharon D. Nelson, Esq. and John W. Simek

As many readers know, we lecture a lot. A whole lot. So we thought it might be interesting to relate the questions we have been asked most often in the past several months. Always fascinating to see what is "top of mind" at conferences and CLEs.

"I've been thinking about cybersecurity - what's most important? A security assessment, penetration testing or employee training?"

Well . . . let's start with penetration testing. For most solo/small law firms, this is probably overkill unless you have major league clients or extremely high value data. In pen testing, you are asking a company to pretend they are the "bad guys" and attack you – it is scary stuff, and tends to be expensive. The company will generally require a "get out of jail" free agreement, saying that they are not liable for any damages resulting from a successful compromises of your network.

A security assessment (sometimes also called an audit) is far less expensive. The assessment is usually done using software tools and involves a thorough review of your network. The result is generally a report identifying your critical vulnerabilities, medium-level vulnerabilities and low-level vulnerabilities. As a rule, it tends to come with a proposal for (at least) remediating the critical vulnerabilities along with the estimated cost. We believe it is wise to do these assessments, using a certified third party cybersecurity company, annually. Many clients and cyberinsurance companies are beginning to require these assessments as well.

There is no getting around the absolute need for annual employee cybersecurity training. It is generally fairly inexpensive and covers the basics of current threats and how to avoid such things as clicking on suspicious links/attachments, going to sketchy websites, giving information over the phone (duped by social engineering), and many other easy-to-make mistakes. A solid hour of good training each year is a small price to pay for educating your employees and creating a culture of cybersecurity.

"What is the best password manager?"

In our opinion, the best password manager is **one you actually use** – because most of you don't use one. Seriously, any good password manager is fine and the selection is largely a personal one. What features do you need? Does the password manager have to automatically fill in website forms for login? Can the password manager store all the various types of data (e.g. Passport, credit cards, prescriptions, etc.) you need? Is the password database stored in the cloud or locally on your own device? Can the password database be replicated and synchronized across multiple devices, including your smartphone?

If you want a little neutral help, check out PC Magazine's review of the best password managers of 2018: https://www.pcmag.com/article2/0,2817,2407168,00.asp. The two highest rated are Dashlane and Keeper, but you should review the feature sets and pricing to see what works best for you.

"Is it really safe to move my law firm data to the cloud – and is it ethical?"

Virtually all cybersecurity experts now agree that the cloud will protect your data better than you will. Is the cloud absolutely secure? Of course not. But do law firms, especially solo/small firms tend to be woefully insecure? Yes, they do.

Most lawyers are using the cloud these days – perhaps for email, perhaps to share files, perhaps because they have Office 365. There isn't a single state bar that has a problem with cloud computing – provided that you take reasonable precautions to comply with your ethical duties. This means asking questions such as:

- Where will my data be stored?
- Is it encrypted at rest and in transit?
- Who holds the master decryption key? (preferable if you do)
- How long has the provider been in business?
- Is the provider accustomed to working with law firms and familiar with legal ethics?
- What happens to your data if the provider declares bankruptcy?
- What happens to your data if you change providers? What format is your data provided in? Is there a charge?
- If law enforcement appears with a search warrant for your data, will your provider notify you right away so you have the chance to file a Motion to Quash?
- Who has responsibility for reporting a data breach should information be compromised?

As you might imagine, there are a lot of questions that you might ask. You can find many useful expert tips for moving your firm to the cloud at https://www.attorneyatwork.com/tech-tips-making-move-cloud/.

"How can I keep up with legal technology? It moves so fast!"

Trust us – we have the same problem. We each read about two hours a day – and we still can't keep up. We have a couple of resources to recommend. We didn't want to recommend a long list, but here's our favorite two resources:

Bob Ambrogi's LawSites blog at https://www.lawsitesblog.com/ Bob keeps up at the forefront of legal technology.

Attorney at Work blog, which offers a good tip each day which may be found at https://www.attorneyatwork.com/. Not all of the tips are legal tech, but all the tips are interesting and many involve technology.

If you sign up for these free resources, you will receive an email each day. The vetting process is very simple – just look at the subject line – you'll know right way if this is a topic you're interested in. If not, hitting the "delete" button is simple.

Beyond these two resources, there are plenty of legal tech podcasts at Legal Talk Network. https://legaltalknetwork.com/ If you are driving to work every day or taking a train/plane/bus, listening to a podcast is a perfect way to learn – and it makes travel time pass faster!

Don't forget CLEs – and ask your colleagues for recommendations regarding speakers who both inform and entertain. Legal tech is hard enough for most lawyers – a few entertaining stories along with the legal tech education is always a good mix.

"Is it safe to open emails as long as I don't click on a link or attachment?"

Generally speaking, yes. You are unlikely to have any malware installation if you use a browser to access your email. The majority of lawyers use Outlook as their email client, which also has safeguards against automatically running scripts. As with all technology, things can change so be sure you are especially careful when opening a suspicious email.

"What is the security software you recommend for smartphones?"

ALL smartphones should have some security software, even iPhones. Many of the major desktop security suites (e.g. Symantec, Trend Micro, Kaspersky, etc.) also have agents for mobile devices. The advantage is that the same centrally managed administration console can monitor desktops, servers and mobile devices. We would suggest investigating Lookout or Sophos for stand-alone installation of security software for mobile devices.

"How do I recognize a phishing email and what should I do with a suspicious email?"

There are obvious red flags to pass on to employees:

- You don't know the sender
- You do know the sender but if you look closely, the address is one letter off (this one happens a lot)
- Nothing in the note seems personal to you
- You weren't expecting the email
- Reference is made to a bank/product/service you don't use
- Words are misspelled
- The grammar is poor
- The email doesn't address you by name
- The message asks for personal information
- There is an attachment which seems suspicious in conjunction with other factors or a link to a website (and no, hovering over the link doesn't necessarily ensure that you will go to the address shown – drive-by malware infections from visiting malicious sites are quite common)

The list goes on and on – you need to advise your employees to be on the lookout for anything suspicious and not to be click-happy! If something about the email doesn't feel "right", you should have them forward the email to your IT or cybersecurity folks.

"What's the most important security tip for 2019?"

Beyond a doubt…DO NOT reuse passwords! The bad guys are now using computer bots to brute force attacks using passwords revealed from past data breaches. If you continue to reuse passwords, there is a high probability that the password will be used against other systems. This is another great reason to use password managers so that you can have unique passwords for every system.

One password you should NEVER reuse is the password you use to log into your law firm network.

"I've heard that Office 365 and Windows 10 are not inherently secure – what can I do to make them secure?"

Default configurations are never good – and Microsoft acknowledges that, though users seem blissfully unaware of it. Microsoft has developed a program called Secure Score. Microsoft first introduced Office 365 Secure Score to help to understand your security position by giving you advice on what controls you should consider enabling, and helping you understand how your score compares to other organizations. As an example, enabling MFA (multi-factor authentication) is worth 50 points. The higher the score the better the security posture. The program was so successful that it has been expanded to include Windows Secure Score since there are also options and features you can enable in a Windows environment. As a result, the program is now called Microsoft Secure Score and includes Office 365 and Windows. Just do a search for 'Microsoft Secure Score' and you'll see information on how to grade and improve your Secure Score.

"What is the most common cause of data breaches and who is behind them?"

Every year, the Verizon Data Breach Investigations Report gives us the most current answer to that question. You can download the report at https://enterprise.verizon.com/resources/reports/dbir/. Hacking is the most common threat, with 81% of the hackers using stolen credentials (ID/password).

More stats that are useful:

- 73% of the breaches were perpetrated by outsiders while 28% involved internal actors (this could mean simple error as well as malicious actions).
- 50% of breaches were carried out by organized criminal groups.
- 12% of breaches involved actors identified as nation-state or state-affiliated.

"What should I do when I get an email with wiring instructions from a client or one of the law firm partners?"

There should always be a verification process – a written policy is a very good idea. If you can walk down the hall to see the person in your office who actually sent the instructions, that's a good way to get verification – and a little exercise. You can also pick up the phone and call the partner or client – but never use a phone number contained in the email about the wiring instructions. Use a number you know to be that of the partner or client.

The same advice applies to requests for W-2 information – this scam tends to peak every year around tax time.

"What are new rules for making passwords?"

New Digital Identity Guidelines were published by the National Institute of Standards and Technology in June of 2017 and may be found at https://pages.nist.gov/800-63-3/sp800-63b.html. First, passphrases are recommended – they are much easier to remember. "Breaker19,you'vegotabearintheair" is a perfectly good choice (for fans of *Smokey and the Bandit*).

While the guidelines call for a minimum of eight characters, most experts are recommending fourteen. NIST says passwords should be allowed to be as long as 64 characters, which we know isn't something lawyers are going to do. Passwords should allow all printable ASCII characters, including spaces, and should accept UNICODE characters too, including emojis. We note with a chuckle that we saw emoji passwords demonstrated on *The Today Show* and no one could remember them just a couple of minutes after making them.

Every time you make a new password, it should be checked against a database of known compromised passwords, so you can't choose one of those. This is slowly being automated as we write. Very soon, this will be standard.

Also, for those of you with security fatigue (and isn't that all of us?), you don't need to have passwords expire without reason. Passwords should only be reset when they are forgotten, if they have been phished or if there is reason to believe that they may have been compromised.

"I do work from home – how do I secure my wireless network at home?"

First, change the default settings of the wireless router. You should change the settings for the network name (SSID), IP address range, administrator ID, password, etc. Next, configure the Wi-Fi to be encrypted. Currently, there are three types of Wi-Fi encryption - WEP, WPA, and WPA2. WEP and WPA have been cracked and there are free tools available to break the rather weak encryption. WPA2 has also been cracked, but vendors have developed patches to improve the security. That means that you should be configuring your wireless router to use WPA2 encryption at this time. The good news is that the WPA3 standard has been approved. We should start seeing products supporting the new standard in 2019, perhaps even by the time this column is published. Keep an eye out and upgrade/replace your wireless router to one that supports WPA3.

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

Anatomy of a Data Breach

by Sharon D. Nelson, Esq. and John W. Simek

"I could have evaded the FBI a lot longer if I had been able to control my passion for hacking."

- Kevin Mitnick (the first hacker to make the FBI's 10 Most Wanted List)

Introduction

Hacking can indeed be a passion, proving that you can outfox governments and big league corporations. The thrill of the chase can be addictive – and the addiction is fueled by the monies to be made.

Breaches come in many variants, far too many to cover in a single article. But there is a general flow to a breach. Since we make a living investigating breaches and remediating the vulnerabilities that caused them, let us take you on an anatomical tour of a typical breach, highlighting some of the common elements.

To make the reading more fun, we have offered up "quotes" from the players typically involved in a breach. Many are taken from real-life incidents.

Hackers: "Let's plan our attack."

Whether there are massive attacks of automated bots looking for vulnerabilities and exploiting them or spearphishing attacks (tailoring a phishing email to a specific target), there is planning. When state sponsored hackers from China attack governmental facilities in the U.S., the planning is intense – and highly coordinated. These hackers are often working in government buildings. Other hackers, primarily cybercriminals, belong to loosely affiliated groups – they are often working together in the ether, not in a physical location.

Many cybercriminals are looking for a known vulnerability to exploit – this was the case with the WannaCry ransomware, which succeeded so well because Windows 7 users hadn't timely patched their operating system.

If you want to, you can go on the Dark Web and buy a vulnerability. It is not quite as simple as an Amazon 1-Click purchase, but it's not hard either. Some hackers will pay big money for a "zero-day" piece of malware (one that has never been used and therefore no specific defenses exist against it). Some will pony up a lot of cash (or cybercurrency) for a previously undisclosed vulnerability, again with a high probability of success.

Do they want to attack through the weak security of Internet of Things devices? Do they want to exploit all the entities, including law firms, which have moved to Office 365 without properly securing it? There are many decisions to make. They involve targets, attack surfaces, tools, objectives, dates, methodologies, etc.

If they are crafting phishing e-mails, the more sophisticated hackers will hire native English speakers to help them – that means that poor grammar and wrong forms will not give them away.

Like the old-time grifters used to say, there's no con without a plan. And part of the plan is not getting caught, right? So you use a sleight of hand. If you're Russian and you want to hide the source of the attack, you do some technical magic and now it looks like the attack came from China. Hackers are all about smoke and mirrors.

Hackers: "3-2-1 – FIRE!"

When it is time to push the button, the hackers involved are usually pretty intense in watching their attack proliferate across the globe – or if they are spearphishing, they are on high alert watching for a response to their bogus or spoofed e-mail. Or they are waiting for an unthinking employee to click on an attachment (containing malware) or click on a link to a website (containing malware).

Some results are fast, some less so. But you can be sure the watchers are riveted, monitoring the results of their handiwork. The truly sophisticated don't even watch. They have automated systems that notify them automatically when a target has been breached.

Hackers: "We're inside. Let's pwn everything we can!"

If the point of the breach is to purloin data, the hackers will try to use their malware to move laterally across your network and "pwn" ('hackerspeak' for 'own') everything they can. Imagine the value of data in a mergers and acquisition law firm. You could sell the data to others or use it yourself to get rich on the stock market. State-sponsored hackers can give their countries a competitive advantage against the U.S. Economic espionage is more and more common.

The longer a hacker is inside the network, the more the hacker learns about the network itself and its users. That knowledge can be a springboard for figuring ways to compromise more user accounts and gain access to more data. One primary objective is to keep the attack hidden.

We haven't made a lot of progress in discovering data breaches. According to the *2018 Ponemon/IBM Cost of a Data Breach Study*, it still takes an average of more than six months to discover a data breach – and the mean time to contain the breach is 69 days. This gives hackers a lot of time to gather your data.

Law firm managing partner: "Oh crap, we've been breached."

'Crap' may or may not be the exact word choice, but we have heard many such utterances. They are generally made in a nervous (sometimes hysterical) voice – and the stress of dealing with a data breach is immediate – and runs throughout the investigation and remediation. The stress is worse if knowledge of the breach becomes public.

If the law firm has an Incident Response Plan, it is the first resource for those within the firm in charge of dealing with the breach. They begin picking up the phone to call the regional office of the FBI, their insurance company, their data breach lawyer, their digital forensics company, their bank, and the list goes on. All 50 states now have data breach notification laws, so those will be carefully read to determine if a report (or reports) must be filed and when.

Rarely, if ever, does a law firm notify clients at this juncture. In most breaches, it is not immediately known what data may have been compromised – and there is natural reluctance to tell clients anything until the investigation is well underway. The exception is when the breach goes public – and then there is little choice but to talk to clients.

Law firm receptionist: "The FBI agents are here."

There is something about the arrival of the FBI agents that unnerves those delegated to meet with them. In our own experience, the agents are polite but somewhat humorless. Understandably, from their point of view, it is a Joe Friday "Just the facts ma'am" kind of meeting.

If it makes you feel better (at least slightly), the agents do not arrive in marked vehicles and they are not wearing the emblazoned FBI jackets. They are also not loose-lipped – you will not find an account of their meeting with you leaked to the press or elsewhere. They are in the business of keeping things confidential.

But be forewarned, it is not their place to do the actual investigation and remediation of the breach – that job belongs to private digital forensics investigators. This seems to disappoint some law firm leaders, who hope that the FBI can "fix the problem." The FBI agents are there to gather data. This is how the government gathers facts which may help everyone, for instance by sharing information about hacking methods, tools, groups, etc. through such vehicles as the FBI's Infragard program.

If there are national security implications to the breach, the FBI may bring in colleagues from other agencies, notably the Department of Homeland Security. At that point, they may go beyond information gathering and take actions – but that is the exception rather than the rule.

Digital forensics investigator: "Yeah, we know how they got in. You pretty much sent them an engraved 'hack me' invitation."

OK, the investigators will probably be more diplomatic. But between themselves, this is often the conclusion they reach – that the client's security was sloppy. It is exceedingly rare for qualified, highly certified digital forensics investigators not to find the cause of the breach, though it may take time. As noted above, the average time to contain breaches is 69 days – 69 days of long, hard, excruciatingly detailed work, with every step carefully recorded.

Progress reports will be given regularly to law firm management. Once it is known how the hackers got in, you will be informed. Remediation steps and their costs will be presented for approval. Given that there has been a breach, there's usually not a lot of deliberating about spending the monies.

Typically, breaches are traced to a long list of possible causes (the engraved 'hack me' invitation), including users clicking on a link in or attachment to an email, sharing of log-in credentials, reusing of passwords, weak passwords, failure to update/patch software, lost or stolen devices, privilege misuse, insecure websites, malicious insiders, social engineering, etc. But at the end of the day, there is generally some kind of malware which must be rooted out of the network – and this process can be time-consuming and complicated.

Longer term recommendations usually include employee training, phishing tests (with consequences for multiple failures, up to and including termination), regular security assessments and penetration testing, in which the security company acts as though it were an attacker.

Law firm insurance company: "We don't cover 'stupid'."

The cyberinsurance world remains the Wild, Wild West. With a notable absence of historical data to guide the industry, even Warren Buffet, CEO of insurer Berkshire Hathaway, is skeptical. He said in May of 2018, "Cyber is uncharted territory. It's going to get worse, not better . . . There's a very material risk

which didn't exist 10 or 15 years ago and will be much more intense as the years go along." He went on to say, "We don't want to be a pioneer on this ... I think anybody that tells you now they think they know in some actuarial way either what [the] general experience is like in the future, or what the worst case can be, is kidding themselves." We could not concur more.

Buffet's views are reflected in more and more cyberinsurance policies, which now often include requirements for security audits and also include language about conforming to industry cybersecurity standards, The case we refer to above because it became known in the press as the "We don't cover stupid" case is *Columbia Casualty Co. v. Cottage Health System*. There are now more cases in the judicial system where insurers are saying the insured did not take the reasonable security steps required by the policy. We certainly know a lot of law firms whose cybersecurity practices wouldn't stand up to some of these new insurance requirements of "best practices" or "industry standards."

Law firm client (whose data was compromised); "We need to reevaluate our association with your firm."

The sound of clients beating a path to the law firm exit door is a scary thought but in light of all the law firm data breaches that have become public, we know that more and more clients are not taking even long-term relationships with law firms as a continued certainty where cybersecurity is lacking.

Ten years ago, only a handful of clients seemed deadly serious about demanding that their law firms demonstrate that they were focusing – and spending money - on cybersecurity. That has markedly changed. Now clients are demanding that law firms fill out security questionnaires and sometimes demanding a third-party audit which certifies that any critical vulnerabilities found have been remediated.

In 2017, the Association of Corporate Counsel upped the ante when it released *Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information*. The gauntlet was effectively thrown down, identifying the standards outside counsel are expected to meet with a hint of "or else."

Law firm management meeting: "Anyone think we need to spend more money on cybersecurity NOW?"

From our foxhole, there is a bit of "We told you so" in seeing law firms, given a well-thought cybersecurity proposal, reject the proposal and then suffer a breach because of the very vulnerabilities that were addressed by the proposal. From our colleagues in the cybersecurity industry, we understand that this happens all the time. It is frustrating. Much of the time it has to do with spending money (hence the subhead above) or simply a wrong-headed belief that "it can't happen here."

On a regular basis, you probably see CLEs advertised focusing on how to get cybersecurity buy-in from law firm management. Data breaches have a marvelous way of getting law firm ostriches to remove their heads from the sand. With perfect clarity of vision, they now see that cybersecurity is an integral part of any law firm's risk management planning. And they do tend to crowbar open their wallets, especially when their clients or their insurance company require various reassurances.

Final thoughts

At the end of the day, hackers want your data or your money and sometimes both. Their motivations are not complex. You may remember the movie "Bonnie and Clyde" and the scene where Clyde announces to strangers, "We rob banks!" Simple, to the point, and said with pride. Hackers, who are also criminals, are generally equally enthused about their work.

When you are up against an expert hacker with a wide array of hacking tools and sufficient funding, you don't have much of a chance. Your best defense is being prepared and making cybersecurity a priority. The hacking community is gunning for you – of that, you can be quite sure.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, cybersecurity and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com

On the Road Again: Secure Mobile Computing

By Sharon D. Nelson, Esq. and John W. Simek

Lawyers are more mobile than they have ever been before but secure mobile computing remains an elusive goal. Wow, have things really changed. Technology has changed with remarkable speed, as have security threats and the "bad actors" who want your confidential data. We connect to our law firm networks from all sorts of wireless networks, at hotels, conference centers, coffee shops, the homes of our friends – even from airplanes now. Many of these connections are free and many are fraught with peril.

It's not just about traveling domestically either. It's a brave new world and crossing the border subjects us to searches of our electronic devices. Lawyers need to be aware of the new rules and how they can continue to keep client confidential information out of the hands of unauthorized individuals.

A great starting point is the National Cybersecurity & Communications Integration Center (NCCIC) tips for secure mobile computing while traveling. There are tips for Holiday Traveling with Personal Internet-Enabled Devices, Cybersecurity for Electronic Devices and International Mobile Safety.

Software

Before we jump into the boring details, let's cover some solutions that should be on your laptop no matter what other technology you use for remote connectivity. It goes without saying that you should have some sort of security software solution installed on your laptop. It should be configured for automatic updates. Security software is no longer just about anti-virus protection and downloading virus definition files. Modern Internet Suite products contain security features such as anti-virus protection, malware protection, firewalls, spam control and anti-phishing. Some products even use artificial intelligence to help protect your computer system. If suspicious activity is detected (e.g. something acting in a similar fashion to malware), the software will stop the action. No definition file needed.

Encryption

Secure mobile computing must contain some method of encryption to protect the valuable personal and client data. We prefer whole disk encryption. This means that everything on the hard drive is encrypted. We don't have to remember to put files into special folders or on the encrypted virtual drive. All too often, humans are in a big hurry and may not save the data in the special protected encrypted areas. Many of the newer laptops have built-in whole disk encryption. To state the obvious, make sure you enable the encryption or your data won't be protected. Also, encryption may be used in conjunction with biometric access. As an example, our laptops require a fingerprint swipe at power on to properly boot. Failure at that point leaves the computer hard drive fully encrypted. A very comforting thought if laptop thieves, who constitute a large club these days, make off with your laptop.

There are even free, built-in alternatives. Even if your laptop doesn't have biometric access or hardware encryption, you're probably using an operating system that includes encryption. If you are an Apple user, File Vault 2 encryption is included with the macOS. However, it is not enabled by default. If you are

a Windows 10 Professional user, encryption is also included for free. Microsoft includes BitLocker encryption with Windows 10 Professional and not Windows 10 Home. Just like File Vault, BitLocker is not enabled by default. BitLocker is only available in the Ultimate and Enterprise editions of Windows 7. You really should be running Windows 10 Professional. You'll need some sort of encryption software if you are running a version of Windows 7 that does not include BitLocker.

Wireless

Wireless is the rage of all the road warriors. There are two basic types of wireless access you'll encounter. The first type is generically termed a "wireless hot spot" and is what you find at your local Starbucks, fast food location, library, hotel or at the airport. You may or may not have to pay for these wireless connection services. Many businesses are offering free wireless as a way to attract customers. Most of these "hot spots" are unsecured. This means that it is possible for your confidential data to be viewed by the customer at the next table or the one sitting on the park bench outside the café.

Does this mean you shouldn't use any of these wireless clouds? If you have a choice, we would say these clouds are best avoided by those who are technology-adverse and don't understand how to operate securely in an unsecured cloud. Read on, and determine whether you can safely be trusted to do what follows. Here are the precautions you should take. See if there is an option to have a secure connection to the cloud. This would be indicated if you use https:// as part of the URL. Typically, the connections are unsecured and do not provide an encrypted session like the https:// connections do.

Be especially careful if you have to pay for the wireless connection. Be wary when you are at the screens that have you input your credit card and billing information. DO NOT enter any of this sensitive information without a https:// connection. Once you've established a connection to the wireless cloud, be sure to use your VPN (Virtual Private Network) or other secure (https://) access to protect your transmissions.

Some hotels may give you a wireless cloud that is already secured. Typically, these wireless implementations use WPA2 (Wi-Fi Protected Access 2) to secure the data. The cloud will be visible to your computer, but you will be required to provide a password before your computer connects. Once connected, your data is encrypted and secure from those not connected to the same Wi-Fi network. However, you should still use a VPN when sharing access to a public Wi-Fi network. The reason is that even if you need a password to connect to the WPA2 Wi-Fi network, it is probably using a pre-shared key (PSK). That means that all devices connected to the same Wi-Fi network are using the same encryption key. Some other device connected to the Wi-Fi could potentially "sniff" the data transmission contents. Using a VPN encrypts the transmission outside of the WPA2 encryption, making the data transmission secure.

While you're at it, turn off Bluetooth whenever you are not using it. You may even want to consider not using Bluetooth at all, especially when traveling to some foreign countries.

Personal Hot Spot

An even better alternative to public Wi-Fi is to use your personal hot spot. Most users will accomplish this by enabling the hot spot feature on their cell phones. When you configure your smartphone, make sure you select WPA2 as the encryption type for the Wi-Fi network. The data connection (e.g. 4G, LTE, etc.) from your phone to the cellular carrier is encrypted. Selecting WPA2 will encrypt the Wi-Fi network, thereby providing a completed encrypted communication channel from your computer through the cellular provider.

Remote Access

We've dealt with some of the more common methods to provide secure communications. Now that you have the secure connection, what's next? E-mail access is pretty simple from most laptops, but what about working on client files? Larger firms will have an environment where you connect to virtual computers. We have a Microsoft Terminal Server environment, where multiple users connect to virtual machines. You connect and login just like you would while you're in the office. You would then have access to all your data just as if you were sitting in your desk chair. Citrix is another technology solution that provides the same function.

Smaller firms typically use something like GoToMyPC or LogMeIn. These products take control of a remote machine and pass keystroke, mouse movement and screen updates across the connection. This does require that the remote machine be powered on prior to you connecting. Be sure that you have a screen saver password set on the computer so nobody can sit at the keyboard at the office and access your computer. Cleaning crews are known to do this! These remote control solutions are very cost effective and all communications are over a secure encrypted connection.

If you use Outlook as your e-mail client connected to an Exchange server, take the extra step and encrypt the communications. You are looking for the configuration item "Encrypt data between Microsoft Outlook and Microsoft Exchange." Don't worry if you are an Office 365 user. The traffic between Outlook and Exchange Online in Office 365 is encrypted regardless of the "Encrypt data between Microsoft Outlook and Microsoft Exchange" setting.

Public Computer Usage

A word of warning here. Be very careful about using a public computer such as those in a public library or business center of the hotel. Even if you are only accessing your web-based e-mail account, the data is temporarily written to the local hard disk. There is also the risk that some keystroke logging software is installed on the computer, thereby capturing everything that you do on the machine.

Does that mean all public computers are off limits? Not at all. It's fine to check the sport scores from the day before, but don't do any sort of business on the machines. Because of the possible existence of keystroke loggers, even using a VPN won't protect the data. The keystroke logger will just capture everything you type, including any passwords. We know it's tempting to use the hotel business center computer to print your boarding pass, but resist the temptation. Once you login to your frequent flyer account, the bad guys will have captured your authentication credentials. They then transfer all of your airline miles to an account they control. Remember…those miles can be worth a lot of money.

Cloud Computing

Lawyers may want to consider moving their practices to the cloud. We have seen a huge movement to the cloud, especially by solo and small firm attorneys. Office 365 has been a huge influencer for cloud adoption. Why move to the cloud? Primarily, because cloud providers tend to have better security practices than most solo/small firm lawyers. Also, having client confidential data in the cloud will protect it from being accessed by Custom and Border Patrol personnel when crossing the border. In fact, the CBP has clarified that they will not access any data in the cloud as part of a border search. Just remember not to synchronize any cloud data to your local electronic device until you are safely back in the United States.

Ethical Duties

Lawyers have an ethical obligation to protect client confidential information. The New York City Bar has reissued an ethics opinion dealing with An Attorney's Ethical Duties Regarding U.S. Border Searches of Electronic Devices Containing Clients' Confidential Information. The digest of the opinion reads:

> *Under the New York Rules of Professional Conduct (the "Rules"), a New York lawyer has certain ethical obligations when crossing the U.S. border with confidential client information. Before crossing the border, the Rules require a lawyer to take reasonable steps to avoid disclosing confidential information in the event a border agent seeks to search the attorney's electronic device. The "reasonableness" standard does not imply that particular protective measures must invariably be adopted in all circumstances to safeguard clients' confidential information; however, this opinion identifies measures that may satisfy the obligation to safeguard clients' confidences in this situation. Additionally, Under Rule 1.6(b)(6), the lawyer may not disclose a client's confidential information in response to a claim of lawful authority unless doing so is "reasonably necessary" to comply with a border agent's claim of lawful authority. This includes first making reasonable efforts to assert the attorney-client privilege and to otherwise avert or limit the disclosure of confidential information. Finally, if the attorney discloses clients' confidential information to a third party during a border search, the attorney must inform affected clients about such disclosures pursuant to Rule 1.4.*

As we've previously mentioned, CBP can't search what you don't have. That's why we recommend using cloud services, especially when crossing the border. Also, make sure you carry business cards and your bar card to further establish the fact that you are a lawyer and searching of your electronic devices requires special handling.

Final Words

The options for secure remote access have certainly changed quickly over the years. Every time we give a presentation on secure mobile computing, the presentation changes. So stay current in your knowledge and take a refresher CLE every now and again. It may be scary to hear of all the new threats and attack surfaces but you can't protect your confidential data if you don't regularly refresh your knowledge. You remember all the references to WPA2 encryption above? Well, it has a vulnerability that has recently been discovered known as the Krack Attack. By the time you read this, it is very likely that a WPA3 standard will have been proposed or adopted. If you feel like cybersecurity moves at warp speed – well, it does.

The authors are the President and Vice President of Sensei Enterprises, Inc., a cybersecurity, information technology and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com

The Basics of Backup

by Sharon D. Nelson, Esq. and John W. Simek

Protecting Your Practice

Is backup a particularly sexy topic? No, but it sure generates a lot of questions when we lecture. And lawyers have begun to comprehend the significance of backing up wisely – especially after the data catastrophes caused by the natural disasters of 2017. Lawyers are increasingly keen to learn how to backup their data well.

Moreover, lawyers are ethically compelled to protect the confidential data entrusted to them by their clients. That means much more than securing their networks from external attacks and other cybersecurity incidents. Ransomware infections could cripple law practices by encrypting data and rendering it inaccessible. Every lawyer needs to be prepared to recover from a security incident, including those caused by Mother Nature.

Backup

Backup is an essential operation for every law firm – and yet, often poorly understood. Having an adequate backup is implicit in the ABA Model Rules for Professional Conduct and their state counterparts, as any legal ethicist will tell you. One of the lawyer's duties is to competently represent clients. How can you do that if your case files and communications are lost? You could have a hardware failure of your server or a disk crash. What if your cloud provider shut its doors, rendering client data inaccessible? Perhaps your laptop is stolen from your vehicle with client data for a pending matter. There are all kinds of situations where you could lose data or not be able to access it. That is where your backup comes into play. Should you have a catastrophe, you would restore data from your backup and be back in business.

A local backup is also a necessity if you use cloud services and your Internet connection goes down. You could certainly take your laptop to a public open Wi-Fi and get to your data that way, but having a local backup of your data is a good idea too. It gives you a safety net should something catastrophic happen to your cloud provider.

These days, the threat of ransomware is foremost in many attorneys' minds, no doubt because more than half of business surveyed have suffered a ransomware attack. For those that have been living under a rock, ransomware is basically malware that encrypts your data with an encryption key that you **do not** have. You must pay the ransom in order to get the decryption key and hence access to your data. The sad reality is that even though you pay the ransom, you may not get the decryption key. The latest statistics are that you will get a valid decryption key in less than 50% of the cases after paying the ransom. The scary part is that we are beginning to see some forms of ransomware that do not encrypt data, but rather destroy it! There is no option to decrypt the data since it no longer exists. Most lawyers have not heard about this terrifying form of attack but once again, backups may be your salvation.

In order to recover from a ransomware attack, backup is your friend. If you are unlucky enough to contract ransomware, just restore your data back from your backups. Of course this implies that you have good backups and have done test restores to make sure you could actually recover from an attack

or failure. Test restores are crucial to verify that the data is restorable and not corrupted. All too often we hear of law firms that have no backup or the backup is corrupted. One solo practitioner, who used a cloud backup, lost five years of law firm data – he had never done a test restore so he never knew that there was anything wrong with the backup. In such cases, you might sue the service provider – but that doesn't get your data back!

External USB Drives

Many solo and small firm attorneys use external USB drives for their backup. That is a perfectly good solution, but disconnect the drive once the backup is completed. Also, you should have at least two backup drives in case one of them is connected at the same time your computer experiences a ransomware infection. We have dubbed this advice "virgin backup" – you must have a backup which is not connected to your network – therein lies your peace of mind.

Hopefully your computer is equipped with a USB 3.0 port, which will allow for faster backups due to the faster transfer speeds versus a USB 2.0 connection. That means you should be only looking at purchasing an external USB 3.0 hard drive. You may want to consider getting a USB drive with built-in hardware encryption. Hardware encryption will ensure that the data is protected when the device is disconnected and powered off. Some external USB drives also come with backup software for no additional charge.

Tape

At this time, we consider tape backup systems to be obsolete. We have come across some law firms that still use tape, but we wish they would convert to a more economical and dependable hard disk type of system. Tape capacity can't come close to the amount of data you can fit on a hard disk. The data transfer rate to tape is also very slow when compared to disk transfers (even with USB). Tape is fragile as well and doesn't have a long life.

Since backing up to tape is not very reliable, it is a best practice to verify the backup after it completes. Verification further increases the amount of time to backup data. Hopefully we've made the case to abandon tape as backup medium and convert to an alternative method.

Backup Appliance

Another solution is to use a backup appliance that is agent-based. This means that you install a software agent on the computer to be backed up and data is transferred over the network to the appliance by using the agent. Think of it as communication software. The agent gathers the data to be backed up and transfers it to the appliance. This communication connection is not seen as a drive letter or a network share, which makes it impervious to ransomware attacks.

Typically, the backup appliance solution is used to backup local servers. The software is configured to periodically take snapshots of the server and stores the backup data on the appliance. In addition, consider sending an encrypted version of the backup data to the cloud, another best practice. Some appliances have the ability to virtualize the server should the actual server suffer a hardware or software failure. As an example, the backup appliances that we implement can take snapshots every 15 minutes and virtualize a server within a few hours. This has been a lifesaver for some of the law firms we work with.

Since the appliance is essentially a server customized for backup, expect to pay up to a few thousand dollars for the initial investment. A lot of the backup appliance providers provide the agents on a monthly subscription basis. The cost may be per agent or based on the amount of data (size of server) that is being backed up. Off-site storage may also be included in the cost or priced on a per terabyte basis. Expect to pay on average somewhere around $100 a month per server being backed up. It could be as low as $50/month or up to $200/month depending on how the provider bases its charge (per device or by size volume). Off-site storage should run around $150-$200 per terabyte per month.

Cloud Backup

Using a cloud-based backup solution will also allow you to restore data following a ransomware attack. Just like the external USB drives, make sure you have at least two backup sets in the cloud.

There are many good backup solutions using the cloud. If possible, you should look to a cloud provider that allows you to control the encryption key used to encrypt the data. Carbonite is a good backup cloud provider that has that capability. A best practice would be to have multiple versions of the backup data in the cloud. That way if one gets corrupted or suffers a ransomware infection, you'll have alternate backup sets to restore from. Another highly reviewed backup provider is Backblaze.

Target Data

Selecting the appropriate technology is just one piece of the backup puzzle. The first thing you need to do is determine what you will back up. If you are looking for a disaster recovery option (total loss of equipment or service), you'll need a method that will allow you to recover quickly and preserve not just the data, but possibly applications as well. You'll probably end up with some sort of backup appliance if disaster recovery is your goal.

Risk Assessment

Once you have determined what needs to be protected, the next analysis is to determine the likelihood of data loss or inaccessibility. How likely is there to be a hardware failure? Perhaps your risk is fairly low if you have new hardware. However, failures can occur beyond hardware issues. Data could become corrupted. Someone could inadvertently delete a file. You could overwrite a file with the wrong version thereby destroying the original contents and of course, ransomware could render data inaccessible.

No matter what the scenario, you should perform a risk assessment and determine action steps to mitigate that risk.

Data Location

Another consideration is data location. Where is your important data being held? Many lawyers still have on premise equipment and keep their data on local storage devices. They just don't trust losing control of the data by putting it in the hands of a third party. Others are using cloud services and confidential client data is out of the lawyer's direct control. Different methods are needed if you have direct access to the data or it resides on some external service.

No matter where the data resides, the challenge is to find it all. You would be surprised at all the places law firm data ends up. Employees take data home. It exists on flash drives. It may be sent as attachments to a personal web-based e-mail account. Spend a little time to inventory all or the data sources. You can't back it up if you don't know you have it. "Dark data" – data a law firm doesn't know it has – has grown by leaps and bounds in recent years. It presents all kinds of risks – you can't protect

that data, you can't back it up and if you don't know you have it, you may fail to disclose it when required to do so by laws and regulations or in litigation.

What about personal devices such as smartphones? You'll have to decide if the information on a personal device is at risk of being lost and should be backed up. This may be a good time to rethink your BYOD (Bring Your Own Device) policy and what devices can access firm data. If you do decide that smartphone information needs to be backed up, there are software solutions to accomplish this. Should you leave the process up to each individual or should you invest in a MDM (Mobile Device Management) system?

How Much?

Finally, how much data do you need to back up? That can radically impact your backup strategy. Hard drive space is fairly cheap these days, but you can't defy the laws of physics. Transfer times are only so fast. You can't make the electrons move any faster. Network speeds will limit the amount of data transfer as well. Perhaps now is a good time to upgrade your network cabling and hardware. If you are only backing up to the cloud, hard drive space is not an issue. However, you will need to know the data volume in order to determine how much the off-site storage is going to cost.

Last words

We worry about backup for lots of reasons. The natural disasters of 2017 were a great reminder of the need for having backups, as many lawyers painfully discovered.

Beyond that, ransomware has been on a wild roller-coaster ride, causing havoc everywhere, including in law firms. Ransomware really is a global epidemic today. The "bad guys" are constantly updating code and discovering new vulnerabilities to exploit. We hope you never have to experience a ransomware event or a system failure. But if you do, make sure you have properly engineered your backup so you can get back in business with minimal effort and pain. Engineering a good backup system is one of the smartest things any law firm can do to protect its confidential data.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, cybersecurity and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com

Are You Ready for a Ransomware Attack?

by Sharon D. Nelson, Esq. and John W. Simek

Ransomware is growing by leaps and bounds. There are reports that ransomware attacks have increased by 748% over the last year. A major international study found that almost forty percent of businesses were hit by ransomware last year. Those are some staggering numbers. Law firms are not immune to ransomware attacks either. Any business is at risk, including the solo attorney. What can we do about ransomware attacks?

In order to understand how to deal with a ransomware attack, we need to understand what ransomware is, how it is contracted, and what impact there may be on your law practice.

What is ransomware?

Let's start with a quick lesson. Basically, ransomware is malware that encrypts your data with a key that you don't have. You can't access the data since it's encrypted and won't be usable until it is decrypted. Effectively, your data is held hostage until you pay the ransom to get the decryption key from the criminals that distributed the ransomware. Normally, there is a countdown timer indicating how long you have to pay the ransom. After the timer expires, the ransom may increase (doubling is not uncommon) or the ability to obtain a decryption key expires forever. There is big money in ransomware. Cybercriminals pocketed more than $1 billion in 2016 alone.

The ransom is requested to be paid in cryptocurrency. Bitcoin is the most requested method of payment. Currently, the average payment is from $650 to $2000. A couple of years ago, you could get by with a $300 payment, but not anymore. At a CLE we were presenting in rural Virginia, a solo attorney told us that he paid $2500 to get the decryption key. Don't worry if you don't know anything about cryptocurrencies. The writers of the ransomware code have very good help files to assist you in creating an electronic wallet and telling you where to go to convert your actual money into bitcoin or whatever other type of virtual currency is acceptable. You probably don't want to pay the ransom these days as you'll only get the decryption key about 50 percent of the time. So much for honor among thieves . . .

You don't even have to be a proficient programmer to take part in the ransomware movement. Some criminal groups are offering ransomware-as-a-service. Instead of charging a fee for the code, they take a portion of the ransoms paid. Typically, they ask for fifty percent of the collected fees.

How do you contract ransomware?

Generally, ransomware is contracted via a malicious attachment or link delivered in a phishing e-mail. It is just amazing how many people will open an attachment from an unknown sender. Some ransomware requires that a second step be taken in order to launch the attack.

One example would be the Locky ransomware. A common way for Locky to be delivered is as a Word document attachment. Once you open the document, the text is unreadable except for a message instructing you to enable macros "if the data encoding is incorrect." Seriously? You shouldn't have opened the attachment to begin with and you certainly shouldn't enable macros, which would launch Locky and start the encryption of your data.

Several ransomware campaigns have been very successful over the years. Locky and Cryptowall have found success for a long time. Their success is due to the regular updates to the code that allow avoidance of detection. Locky has even been updated to support 30 different languages meaning it can target specific countries and the ransom demand will be understood.

Ransomware has morphed

As previously mentioned, ransomware is normally invoked by opening a malicious attachment or link. That thinking changed in May of 2017 when the WannaCry ransomware attack spread like wildfire across the globe. WannaCry "was easily the worst ransomware attack in history," says Avast's Penn. "On May 12th, the ransomware started taking hold in Europe. Just four days later, Avast had detected more than 250,000 detections in 116 countries."

The really scary part about WannaCry is that it is the first ransomware attack that spreads across devices on the network WITHOUT any user interaction. No clicking. No opening of attachments. To be technically correct, WannaCry is classified as a worm because of the self-propagation. WannaCry exploited a vulnerability in Microsoft's implementation of the SMB (Server Message Block) protocol. Microsoft had already issued a patch for the vulnerability, but many people hadn't installed it yet. Lesson one…patch your software as soon as possible.

Another reason WannaCry spread so quickly is that many companies were allowing port 445 (the port used by the SMB protocol) through their firewalls, thereby exposing themselves to the Internet. Lesson two…don't configure your firewall to allow traffic that isn't needed.

According to Kaspersky Lab's APT Trends report for Q2 2017, the next big threat facing the enterprise is destructive malware **disguised** as a simple ransomware attack. That threat is already here. We first saw it with the WannaCry attack and then again in June with the NotPetya (also known as ExPetr) attack. It is alleged that both attacks were nation-state backed. Even though the attacks were originally thought to be typical ransomware campaigns looking for money, further research determined that the real goal was to destroy data. Specifically for NotPetya, analysis of the encryption routine would not allow decryption of the victim's data even if payment was made for the key.

Business impact

To bring things closer to home for the legal profession, it is believed that a NotPetya attack is what brought DLA Piper to its knees and virtually shut down the law firm for days. Some of the shutdown was done as a precaution, but DLA Piper's e-mail was "offline" for several days. As most of us know, e-mail communications is critical to a law firm.

Further, cybersecurity company Malwarebytes found that as many as one third of small to medium businesses were hit with ransomware last year. In addition, one in five had to shut down operations immediately. Not a very pleasant experience if you are the unlucky one to get hit.

Prevention

Obviously, the best thing is not to be the recipient of a ransomware attack at all. We believe that is the ostrich in the sand approach. Employees are human beings and somebody is going to do something they shouldn't do at some point. Ransomware is constantly evolving and taking advantage of vulnerabilities we don't even know exist. Our belief is that we need to be prepared for the inevitable attack and position ourselves in the best way to recover.

One of the first steps would be training. Since a very large portion of the ransomware attacks happen as a result of a phishing e-mail, training employees to recognize those e-mails is a good thing. Some are fairly obvious with misspelled words and poor grammar, but don't count on that to be the only sign. We've seen some very good phishing e-mails that have no errors and appear to come from someone we know. There are several free services that can test employees with phishing e-mails. Take a look at the free phishing services available at OpenDNS, Duo Security or SonicWall.

As previously mentioned, another step is to install all updates and patches as soon as possible. Of course your computer operating systems and software should be updated, but don't forget about the network components as well. Router and firewall manufacturers also distribute updates for their products. Make sure you install them too.

You should also have some sort of security suite installed. The modern day security suites include features such as anti-virus, anti-malware, firewall, anti-phishing, etc. There are other technologies you can utilize to reduce your chance of a ransomware attack. One very simple step is to practice the concept of least privilege mode. Users should have the least amount of permissions required for them to do their job. Unfortunately, we see far too many firms configuring user IDs with administrator access. Avoid this temptation and only logon as an administrator when absolutely necessary. You should also consider restricting user IDs to prevent installation of applications. We guarantee that move will not be very popular, but it will significantly reduce your chance of any ransomware attack being successful.

Recovery

No matter how much training you do or how much technology you implement, there is no solution which will stop a ransomware attack 100% of the time. That means we must operate on the assumption that some data will get encrypted or be destroyed at some point. It's not a question of preventing the attack, but being able to recover from it. You could always pay the ransom (assuming you have requisite bitcoins available within the time period), but that does not ensure you'll even get the decryption key. Paying the ransom also encourages the cybercriminals to continue ransomware attacks.

However, some companies may elect to pay the ransom - as did the Hollywood Presbyterian Medical Center in Los Angeles following systems getting infected with the Locky ransomware. Allen Stefanek, CEO of the hospital said, "The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key."

Backups are your friend. Having a backup of your data unconnected from the network allows you to recover from a ransomware attack. If your data does get encrypted, you can just restore from your backup. However, the important part is to make sure your backup solution is engineered properly. We'll run through a few of the choices here.

Many solo and small firm attorneys use external USB drives for their backup. That is a perfectly good solution, but disconnect the drive once the backup is completed. Also, you should have at least two backup drives in case one of them is connected at the same time your computer experiences a ransomware infection. Using a cloud-based backup solution will also allow you to restore data following a ransomware attack. Just like the external USB drives, make sure you have at least two backup sets in the cloud.

Another solution is to use a backup appliance that is agent-based. This means that you install a software agent on the computer to be backed up and data is transferred over the network to the appliance by using the agent. Typically, the backup appliance solution is used to backup local servers. The software is configured to periodically take snapshots of the server and stores the backup data on the appliance. In addition, consider sending an encrypted version of the backup data to the cloud. Some appliances have the ability to virtualize the server should the actual server suffer a hardware or software failure. As an example, the backup appliances that we implement can take snapshots every 15 minutes and virtualize a server within a few hours.

Last words

Ransomware really is an epidemic today. The "bad guys" are constantly updating code and discovering new vulnerabilities to exploit. We hope you never have to experience a ransomware event. But if you do, make sure you have properly engineered your backup so you can get back in business with minimal effort and pain.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, cybersecurity and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com

How Secure is Office 365? What Lawyers May Not Know

by Sharon D. Nelson, Esq. and John W. Simek

Can Office 365 "Go Down?"

Oh yes, it can. And it most certainly did on April 6, 2018. The outage was experienced in Europe, notably the U.K. as well as in Japan and other regions of the world. As one British newspaper noted in typical fashion, "Microsoft's Office 365 service is suffering widespread borkage across Europe, again." We do love 'Brit-speak.' Another newspaper said "It would appear that Redmond has opted to secure user data by, er, removing access to it entirely. Clever."

An unhappy customer wrote "Get this sorted – not been able to access account at all and working from home. Losing business here!"

Pete Banham, cyber resilience expert at Mimecast, commented: "Microsoft Office 365 was hit with major downtime on Friday, with customers around the world unable to access their services or admin portals. An operational dependency on the Microsoft environment creates business risks that need be addressed." He went on to say that entities need to consider a cyber resilience strategy to allow them to recover from such an outage.

To Microsoft's credit, it announced later the same day that it had fixed the authentication problem. Certainly, it didn't solve the PR problem emanating from all the users who couldn't login.

That certainly made us wonder how long an American law firm would be able to tolerate an Office 365 outage. This is an unsettling thought to many law firms which never thought about Office 365 being unavailable to them.

Creating a cyber resilience strategy

We could write an entire article for creating a resilience strategy, otherwise known as a business continuity plan. If Office 365 has a problem, how does a firm remain functional with e-mail, preparing documents, etc.? This is the point at which you plan to fail. Our recommendation is to use other services that integrate with Office 365. While there are many alternatives, we'll give a few suggestions to keep you running during an Office 365 outage.

E-mail is now a required service for any law firm. Microsoft has a lot of redundancy for Office 365, but we've already seen some major failures. Consider routing your e-mail flow through a service like Mimecast or Proofpoint. Should Office 365 (or hosted Exchange) go down, you can still receive and send e-mail just like you normally would. Once Microsoft comes back up, the "offline" activity is synchronized with Office 365. You'll need to work with your IT folks to get the configuration right, but it is possible to still operate during an Office 365 failure.

File access is another concern for continuity. You can control which OneDrive files are available offline. Access to the Office software (Word, Excel, etc.) isn't an issue since part of the Office 365 subscription is to have local installs of the software.

Other Office 365 services such as SharePoint may be more difficult to engineer offline access. Most firms will be just fine with e-mail and file access. The good news is the extended failures of Office 365 are very rare.

Are you responsible for securely implementing Office 365? In a nutshell, yes.
Lawyers look at us blankly when we ask, "How secure is your implementation of Office 365?" But it is a question posed by Microsoft itself. Let us offer a small tidbit from Microsoft's "Introducing the Office 365 Secure Score" web page:

"Ever wonder how secure your Office 365 organization really is? Time to stop wondering - the Office 365 Secure Score is here to help. Secure Score analyzes your Office 365 organization's security based on your regular activities and security settings and assigns a score. Think of it as a credit score for security."

Office 365 isn't magically secure out of the gate. It needs some help from your end. Secure Score looks at the Office 365 services you use and then looks at your settlings and activities before assigning you a score that represents the quality of your security practices.

When we get a new client that is using Office 365, it is standard practice now to run "Secure Score." And the results are usually dreadful. You don't have to reach the pinnacle here – as we always say, the object is to "get to good."

While we don't know the exact percentage of law firms using Office 365, we do know that lawyers are flocking to it in ever-increasing numbers, at least in our experience. Our best guess is that 35-50% of law firms are now using Office 365,

with many more planning a migration to Office 365. So making sure Office 365 is secure is a very big problem in the legal sector.

Attacks against Office 365

Microsoft is very much the victim of its own success. As soon as a large portion of the marketplace turned to Office 365, the bad guys went on the attack. There was the infamous “KnockKnock” botnet attack that was designed to target Office 365 system accounts, which tend to have elevated privileges.

Criminals employing ransomware attacks began to target Office 365 as well – and the attackers were both lone wolves and organized criminal gangs. Cerber ransomware targeted Office 365 and flooded users’ mailboxes with an Office document that released malware via macros.

Collaboration tools can be a source of danger. Using Office 365 with SharePoint Online or OneDrive for Business, ransomware can spread across multiple users, systems and shared documents. One point of entry can cause a domino effect, giving attackers quick access to data, e-mail and networks.

Microsoft has duly noted the threats and, in April, unveiled an Attack Simulator for Office 365 Threat Intelligence. This phishing attack simulator builds on the work of Office 365 Threat Intelligence, released in 2017, which allows IT pros to analyze threats in near real-time and to set up custom alerts. Just Google “Office 365 Threat Intelligence” and see what’s possible. The dark side of reading about it is realizing the full extent to which Office 365 is under attack.

More about Secure Score

In light of the torrent of attacks on Microsoft Office 365, Microsoft has provided, through Secure Score, recommendations for its customers to improve the security posture of access to its service, reducing risk at the same time. There is no silver bullet nor does Secure Score give you an absolute measure of how likely you are to have a data breach. But it does help assess the extent to which you have adopted security controls which can help prevent data breaches.

Rather than reacting or responding to security alerts, Secure Score lets you track and plan incremental improvements over a longer period of time.

While some of the changes to Office 365 for improving security occur behind the scenes, like auditing or reviewing reports weekly, others are more time

consuming and noticeable to users when implemented, like enabling Multi-Factor Authentication (MFA) or implementing a Mobile Device Manager (MDM).

Microsoft takes the guess work out of achieving these security-minded goals by providing a checklist of tasks and instructions on how to complete those tasks. Once implemented, the secure score will go up. The default score after just implementing Office 365 is 27 and the highest score you can achieve is 450. Our recommendation is to shoot for a score of 250 or better, which will help to increase the security of your data stored within Office 365 and reduce the potential risk of a data breach occurring.

Microsoft charges $1.40 per user / per month for Multi-Factor Authentication, $6.00 per user / per month for the Mobile Device Manager (MDM) called InTune, and Advanced Threat Protection (ATP) costs $2.00 per user / per month.

These are not major costs for most law firms and initial costs for configuring these security measures is not extreme, perhaps in the 10-15 hour time frame for a small firm.

General Data Protection Regulation

The EU's General Data Protection Regulation become effective on May 25th, to the consternation of many entities, including law firms, which were not prepared for the very strict requirements of the GDPR. And be aware that violations of the GDPR carry hefty fines.

If you have European Union clients, or store or process data of EU residents, it is past time to roll up your sleeves and make sure you are GDPR compliant. New features in Office 365 can help you meet the strict GDPR privacy requirements. While this is a complex subject, Microsoft walks you through the key changes under GDPR and the implications for Office 365 users at https://www.microsoft.com/en-us/TrustCenter/Privacy/gdpr/default.aspx.

On the plus side, Office 365 meets requirements specified by ISO 27001, HIPAA BAA and FISMA, users own and retain all rights to the hosted data, users can view a map of where the data resides, and there is limited access by Microsoft database administrators. Microsoft has done a good job with compliance – much harder is fending off the bad guys who want your data.

Final thoughts

Once again, we caution that there is a difference between IT and cybersecurity. A lot of perfectly good IT consultants can get you up and running on Office 365. But can they get you up and running securely? Most law firm managing partners seem unaware of the possible security dangers that come with Office 365. They want to "set it and forget it." It is clear that this worries Microsoft, which has really begun an extensive campaign to wake organizations up to the security risks (and increasing threats) that may come with Office 365.

One wonderful resources provided by Microsoft is an "Office 365 security roadmap: Top Priorities for the first 30 days, 90 days, and beyond." Again, just Google it. This is one of the resources we've found – and a roadmap is exactly what law firms need.

Now that Office 365 has such a big bulls-eye painted on its figurative back, we applaud Microsoft for taking a hard look at security concerns and trying to address them. But this is a dance that requires a dancing partner and those who use Office 365, especially lawyers, have a duty to make sure they are aware of potential security problems and doing their best to beef up their security posture.

Given the dangers that this article has identified, the time for investigation and action is now.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, cybersecurity and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com

Practical Cybersecurity for Law Firms: How to Batten Down the Hatches

By Sharon D. Nelson, Esq., John W. Simek and Michael C. Maschke

Setting the stage

We're quickly approaching 2018 and a week doesn't go by without another variant of malware causing havoc across the globe. First it was the WannaCry ransomware worm, which infected more than 230,000 computer systems in over 150 countries demanding ransom payments in exchange for the decryption of files. More recently, a new variant using code from the Petya ransomware (named "notpetya") struck first in Ukraine followed by other European countries and disabled critical utility services such as the radiation monitoring system at the Chernobyl Nuclear Power Plant, as well the affecting the countries' banks and metro systems.

What caught the attention of lawyers was that an apparent infection in one of DLA Piper's European offices brought the law firm's normal operations to a halt. As we write, the extent of the damage is still unclear.

The times have changed since Cryptolocker first ran wild in 2013, but the results are still as devastating. The costs of ransoms have significantly gone up from a few hundred dollars to the $1,000+ plus range now for the decryption key to unlock the affected files – and more than half of those who pay up do not receive the decryption key. So much for honor among thieves!

Ransomware has continued to evolve and is the primary security concern for businesses of all types and sizes.

How do you protect your firm from ransomware, malware and other cyber threats? Before we get started, as we say all the time (and it rates all caps), **THERE IS NO SILVER BULLET THAT PROTECTS AGAINST ALL RANSOMWARE.** Or all malware for that matter. If a vendor promises you a 100% solution, you are being sold a bill of goods.

Backups

Backups are key. Backup all of your data. Don't forget to periodically conduct a test restore of the data and make sure your backups are impervious to ransomware – either backed up in the cloud or agent-based (talk to your IT provider to learn more) Backups should be encrypted with a user-defined encryption key, whether on-site, off-site or stored in the cloud. If using a cloud vendor, the vendor should not have access to the decryption key. Encryption should be treated as a must – no questions about it.

The simple solution for most solo/small firm lawyers? Use an external USB hard disk. Unplug the external USB hard disk after the backup job completes. Just make sure you have at least two USB hard disks and rotate them in case you are attacked while one disk is connected.

Passwords

Next up, passwords. Develop a password policy. The recommendations for password policies have recently changed. We still live in a password driven world, but the final guidelines from the National

Institute of Standards and Technology (NIST) for the federal government have now been published – see SP 800-63-3: Digital Identity Guidelines which you may find at https://pages.nist.gov/800-63-3/.

While this publication applies to government agencies, it represents new thinking that is sure to be embodied in the NIST Cybersecurity Framework, draft version 1.1, which is in the process of being finalized as we write – we expect the Framework to be finalized by the time this article is published. NIST is phasing out the requirement of periodic password changes – which has been the foundation of password policies for many, many years. Other recommendations include using a length of a least eight characters or more and choosing a passphrase rather than a "password." Some applications and devices allow users to include spaces and even *emojis*, which users can now include when setting their passphrase. As always, do not use dictionary words as these are easy to brute force and please, please force computers to require screen-saver passwords and ensure that passwords are required after a reasonable period of inactivity. Newly included is checking all passwords against a database of known compromised passwords, which will of course eliminate all of the dreadfully easy passwords that users are so fond of employing.

Users should never share their password, write it down or reuse the same password anywhere. It is particularly important that credentials used to access a law firm network **never** be used anywhere else. The use of a password manager can make this task quite easy. Consider enabling two-factor authentication (2FA) when available. Biometrics alone is not a good solution – once your biometrics are owned, they will always be owned. Remember the 5.6 million fingerprints stolen in the U.S. Office of Personnel Management data breach? You can't change your fingerprint.

A password policy should be part of an overall comprehensive security program, which should also encompass an incident response policy, disaster recovery plan and social media policy to name a few.

Patches and updates

Firms need to prioritize efforts to keep hardware and software as current as possible. Keeping up-to-date doesn't always have to cost money – see Windows Security Updates. You don't need to be first in line for the latest and greatest, but don't be the last in line either. Once software becomes unsupported, it is unethical to use it because it is no longer receiving security updates and is vulnerable to attacks. In January 2017, Microsoft stated that Windows 7 is so outdated that patches can no longer keep it secure. Extended support ends 1/13/20, so the operating system will not get any further enhancements and will receive security updates only. What does this mean? It is time to plan an upgrade to Windows 10 if you haven't migrated already. Windows 10 security is leaps and bounds better than what Windows 7 provides.

Firms need to apply patches **as soon as they are available** to reduce the vulnerability to attack or compromise. A perfect example – "notpetya" ransomware – attacks a vulnerability of Windows' Server Message Block (SMB) which is first believed to have been developed and exploited by the NSA – released by hackers in April 2017. Microsoft released a patch to address this security vulnerability in March of 2017, so if a computer system hasn't been updated with security updates since then, it could be vulnerable to this ransomware variant. If you have a Windows Domain environment, have your IT provider configure Windows Server Update Services to download and push out Windows Security Updates to all of your client computers and servers as they are released – a free solution to keeping your operating systems updated.

Encryption

Encryption, once just technical-jargon or something the German World War II Enigma machine used, is now becoming the de facto recommendation from cybersecurity companies. Why? It's no longer cumbersome and time-consuming, but is cheap and easy to set up and use (and maybe ethically required for attorneys – see the ABA's Ethics Opinion 477 (May 11, 2017) on encryption of attorney-client email. Your laptop should be protected with whole-disk encryption – no exceptions. Ditto for any external USB flash drive or hard drive used to store firm information. Stolen and lost laptops are one of the leading causes of data breaches. Many of the newer laptops have built-in whole-disk encryption. To state the obvious, make sure you enable the encryption, or your data won't be protected. For others, Windows BitLocker and Apple FileVault II are free encryption options included with Windows and macOS systems – there is no excuse for not using this free protection.

Also, encryption may be used in conjunction with biometric access. As an example, our laptops require a fingerprint swipe at power on. Failure at that point leaves the computer hard drive fully encrypted.

The same applies to mobile devices - encrypt, encrypt, encrypt. For modern phones – just enable a PIN or password lock code. We recommend six or more characters. Yes, if you use an Apple iPhone, the recommendation is still the same as these devices are not inherently more secure than other devices. You would not believe how many users (and attorneys) still believe that Apple products aren't capable of contracting malware. Apple itself refutes that thought. For the Samsung Galaxy S8, users can use a fingerprint, iris scan or facial recognition (don't use the selfie – this form of 'protection' was compromised within 24 hours!). And don't forget anti-malware software on your mobile devices, such as Sophos, Lookout, Kaspersky or McAfee – ransomware attacking mobile devices is on the rise.

Sometimes convenience causes issues. Providing remote or mobile users with access can create more vulnerabilities than you might realize. To combat this, mandate that all work-related Internet sessions be encrypted. Prohibit the use of public computers and unsecured open public Wi-Fi networks. Access to the office network must always occur through the use of a VPN, MiFi, smartphone hotspot or some other type of encrypted connection. For users that need to connect directly to their work computer, use an encrypted remote control solution such as Citrix, LogMeIn or GoToMyPC. The setup of this kind of software couldn't be any easier and we've seen many attorneys accomplish this on their own.

Employee security awareness training

Malware loves to prey on uninformed users. These victims are the primary cause for the continuing propagation of malware infections, with users clicking on things that they shouldn't be. Why, you might ask? Curiosity, fear, urgency, recognition (such as being named for an award) are generally recognized as the top four motivations for clicking. Over 91% of all hacking attacks begin with a phishing e-mail, which is why it's imperative that you train all of your employees.

Sadly, one of the most often-overlooked aspects of an organization's security readiness is end-user training. It is just as important that your employees know what not to click on as it is to have security software installed to help prevent malware outbreaks. Firms should provide mandatory social engineering and safe computing awareness training to everyone at the firm at least once a year. And make it mandatory!

Technology alone cannot protect your data. The greatest vulnerability comes from your greatest asset - the folks who use your network. Cyberattacks are successful because someone usually did something

stupid like clicking on a link, opening an e-mail attachment, or verifying an ID and password when they shouldn't have. With education and practice comes a more informed and safe user. Look into services that provide phishing assessments, such as Duo Insight (www.duo.com/resources/duo-insight) as a way to test and educate your employees against phishing e-mails. Integrating this testing into annual training is a great way to get your employees to learn, to have a fun competition and to identify those employees that may need some extra "attention" and practice. By the way, a single training session has been shown to reduce the risk of a successful phishing attack by 20% - not a bad return on your money.

Technical solutions

You can also augment your training with technical solutions. There are e-mail scanning services such as Mimecast, which convert attachments into a "safe" format such as PDF. There's also an option to scan URLs in messages and warn of any suspicious links.

There are some free and not so free solutions that your firm can implement to increase your security posture against ransomware and other malware threats. Much of what we describe is probably included in the software that your firm has already purchased. It is just a matter of turning the security settings and requirements on. Our list of security recommendations could fill a book, but we have tried to include the primary essentials above.

Doing nothing makes no sense - you are just begging to be "owned" by the next piece of ransomware or malware. By implementing some of the solutions described above, you are doing your "due diligence" to batten down the hatches, protecting your firm from becoming the victim of the threats that will continue to wreak havoc for the foreseeable future. Cybersecurity is a moving target – as threats morph, so will the defenses – keeping yourself educated on information security issues is a very high priority for all lawyers.

The authors are the President, Vice President and CEO of Sensei Enterprises, Inc., a legal technology, cybersecurity and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com

Security Awareness Training for Law Firm Employees

by Sharon D. Nelson, Esq. and John W. Simek

Introduction and stats

Sadly, your greatest asset – your employees – are also the greatest threat to your cybersecurity. We know this because we regularly see data breaches and ransomware infections caused by click-happy employees. You also have rogue employees determined to use their own devices, go where they want on the Internet, irrespective of firm policies. When we train them, they tell us that they are scared – and you know what? That means we did our job. One of the great fallacies that employees believe is sometimes called "The IT Shepherd" – they simply have faith that the flock (employees) is protected no matter what they do by the shepherd (technology). You need to make them understand that no technological defenses are ironclad.

Let's look at a few statistics. The Computing Technology Industry Association (CompTIA) released the results of a study of 1200 full-time employees in October of 2015. 63% used work mobile devices for personal activities. 94% used mobile business devices to connect to public Wi-Fi networks. 78.5% used public Wi-Fi to check work e-mail and 60% access work documents.

45% have never had any cybersecurity training from employers. 41% don't know what 2FA is. If you don't know, it is two-factor authentication, a more secure way to protect data than using a password alone. 27% know the name 2FA but not how it works.

When researchers salted 200 unbranded USB drives in public, at airports, coffee shops, and parks in Chicago, Cleveland, San Francisco and Washington D.C., 17/% were picked up and used. The flash drives had a trackable link and a text file to tell them to mail an e-mail address. Even IT workers did this – and they should know better!

The Association of Corporate Counsel published *The State of Cybersecurity Report* in December of 2015: Over 1000 General Counsels responded. The dismal result of the survey included the fact that only 1 in 3 track attendance at mandatory cybersecurity training, only 19% give a test, and only 17% have "simulated security events."

Who should do the training?

Certainly not law firm owners. Even if they think they know something about cybersecurity. The biggest hammer is a third-party consulting firm that clearly knows what they are talking about and can answer a fusillade of questions, which generally come fast and furious during training sessions. They bring credibility with them because of their credentials.

If you are an Am Law 200 firm, you are likely going to hire one of the big guns with a hefty price tag. If you are a smaller firm, there are likewise plenty of smaller companies who do cybersecurity training. You want a company that has something of a specialty in training. Hopefully, they have sample phishing e-mails and tests they can give your employees to demonstrate that they are aware of security risks. If an employee repeatedly fails such tests, is that really an employee you want around sensitive data?

Using paper manuals to train is worthless. Online training is not as engaging or effective (our opinion) but 32% of employers use it. In-person group workshops seem to work best. And for heaven's sake,

don't bellyache about the loss of billable time. If you think training is costing you money, just think about what a data breach would cost you – that may put it in perspective.

Training Tips

It sounds silly, but make training (as much as you can) fun. Encourage interactivity – make sure you ask your outside training company HOW they train. You want to hear about sample phishing e-mails, post-training testing, on-the-fly interactive responses as to whether an e-mail shows any evidence of being a phishing e-mail (the number one way law firms are breached). Better yet if you hear that they make a contest out of it, have a whiteboard to list the phishing methodologies they discover – even giving out small prizes. Use real life scenarios. They should tell stories. They may have attendees watch short security videos from YouTube (Sophos makes great ones). We love their tag line: "Skip the book and just watch the movies." And they are right – this is a vital part of effective training.

Time of day? Best done in the morning, when folks are most alert. Spring for breakfast and keep the coffee coming. Cybersecurity can be mind-numbing if not done right.

Make it mandatory? Absolutely. Take attendance. When we trained at one law firm, the managing partner told us he had sent around a memo stating bluntly that the training was mandatory and that he would be at the training and expected to see everyone from the firm there. Splendid idea –and everyone did indeed show up.

How often should you train? At least annually. Threats change and defenses to threat change. Both technology and security policies change. You should assess these changes and your security policies on a regular basis to stay ahead of the curve. You can never "set it and forget it" in cybersecurity.

One famous story that may give you pause: Weeks after falling victim to a data breach in 2015, JPMorgan sent a fake phishing e-mail, which 20% of its employees clicked on. If your results are anything like that, you are in desperate need of cybersecurity training for your employees. JPMorgan got the point – having spent $250 million on cybersecurity in 2014, it vowed to double its cybersecurity budget to $500 million over the next two years.

Physical security

Trainers should be talking about physical security too – not leaving files in stacks around the office, being aware of strangers in the office, etc. One of our friends dressed as a custodian and followed a real custodian right into an office building and got into a law firm. Easier than you think. The infamous "office creeper" in the D.C. area during 2015 got into all sorts of "secure" buildings, once getting into a law firm. She was a standard issue thief, taking money from drawers and purses, lifting laptops and cameras which were easy to pawn. But what if she had been after data?

She got through building security by piggybacking and tailgating. Your trainer will explain those terms if you don't know them. And we're betting most readers do not.

Don't be stupid!

This is the essential message of training. Above, we told you about "salted" flash drives in public places. That's called "baiting" – and people fall for that tactic all the time.

Likewise, if you know that another employee is engaging in insecure behavior, you should inform a supervisor. "See something? Say something" doesn't apply just to possible terrorism, but to cybersecurity as well.

Encryption

Every training session is going to include encryption. Not the math, which employees don't need to understand, but the critical need for encryption to protect confidential data. They will learn about encryption on all of their devices and e-mail encryption. There was a day when encryption was costly, cumbersome and a royal pain, but those days are long gone. It is now cheap, simple and easy. More and more ethicists are stating that lawyers should use encryption "where appropriate" – which is pretty much anywhere that data which ethically must be protected exists.

Don't be mad at your employer!

Employees dislike many aspects of information security. A good trainer will have your back on this one. They will explain why your security policies are needed and why they must be enforced. They'll talk about how the firm may protect its data through application whitelisting, logging of certain events, installing software or hardware that "reports" when certain files (or a certain large number of files) are accessed. They will talk about the dangers of bringing your own device, bringing your own network and bringing your own cloud. They will explain why such things may be forbidden or why they are tightly managed.

They will explain if your technology prohibits employees from opening attachments without asking for the attachment to be released by your IT or information security department. If you control where they go on the Internet, they'll explain that too. They will explain why employees have to give up their beloved (name your software of choice) because it is no longer receiving security updates.

Trainers explain the importance of strong passwords, especially log-on, screen saver and financial credentials. They will encourage the use of two-factor authentication where it is available and they will report on the new Carnegie Mellon studies showing that password length is more important than complexity, which is agreeable news since it is easier to remember a lengthy passphrase than a complex password. There is a new draft document from the U.S. National Institute for Standards and Technology (NIST) which recommends password length over complexity. The rules keep changing, don't they? But that too is why you train on a regular basis.

And trainers will preach the value of encrypted password managers – darn near a necessity if you are going to follow the cardinal rule of not reusing passwords everywhere which often leads to one breach compromising your security, and that of the law firm, in many places rather than just one.

Social engineering

People who are experts at penetrating businesses through social engineering say it generally takes them less than an hour to get into your network. We are so anxious to be helpful. Your employees need to know that Microsoft Tech Support will never call and ask for access to their machine (yes, we've seen lawyers duped). They also need to understand that someone who calls and says they are from your IT company and need log-in credentials to fix a problem may not really be from your IT company, even if they know the company name.

Phishing

As we said before, phishing is the easiest way into law firms. Even good enterprise anti-malware software doesn't catch everything – and there are plenty of zero day (no known defense) exploits sold on the Dark Web every day. Lots of studies have shown that roughly 20% of phishing e-mails will be opened.

The worst threat comes from targeting phishing attacks, where the hackers are specifically targeting your law firm. Law firms are at a disadvantage here – so much legal data is public. A hacker may know what cases you are involved with, who the attorneys are, which courts cases are in, etc. And they can spoof the e-mail address of an attorney or a court – how many folks can resist opening something that appears to come from a court?

Law firms are also at a disadvantage because they are "honey pots" – they hold the data of so many clients. Hackers may do a little research on the firm's website or on an attorney's LinkedIn page where they may find personal information that they can insert into a targeting phishing e-mail. Trainers will get them to PAUSE, THINK, INSPECT and REPORT before clicking on any attachment or links in the e-mail.

There are obvious phishing clues to pass on to employees:

- You don't know the sender
- You do know the sender but if you look closely, the address is one letter off (this one happens a lot)
- Nothing in the note seems personal to you
- You weren't expecting the e-mail
- Reference is made to a bank/product/service you don't use
- Words are misspelled
- The grammar is poor
- The e-mail doesn't address you by name
- The message asks for personal information
- There is an attachment which seems suspicious in conjunction with other factors or a link to a website (and no, hovering over the link doesn't necessarily ensure that you will go to the address shown – drive-by malware infections from visiting malicious sites are quite common)

The list goes on and on – you need to advise your employees to be alert to anything suspicious and not to be quick to click!

If they end up with malware, they may not know it. But some possible signs might include, sudden slowness of devices, strange messages appearing on the screen, the inability to open a file, machine crashes, running out of hard drive space, a high volume of machine activity, suddenly having a new browser home page or tool bar the employee didn't install, new programs appear that start automatically, etc.

Ransomware

Ransomware is an international epidemic. Your employees need to understand that it is usually contracted via phishing e-mails. Click on a link in the e-mail or an attachment and the malware is downloaded invisibly irrespective of what you see on the screen. Then it sets about encrypting the firm's data, file by file. If the backup is connected to the network at the time, it will encrypt that too.

Employees really need to understand how dangerous ransomware can be, how prevalent it is, how the ransom to get your data back is more and more expensive – and that you are out of business until you slog through trying to figure out how to get sufficient funds in bitcoins (which the hackers generally want as payment) – and then there is a delay after receiving the decryption key in restoring the files (assuming you do in fact get the key).

While you can be protected from ransomware by having a properly engineered backup, if you get ransomware, you still have to live through some period of time while the files on an unaffected backup are restored. And we are now seeing ransomware on mobile devices, including phones – most from downloading apps from unsanctioned app stores, a very common practice among employees!

Business e-mail compromises

These are also known as CEO scams and the FBI reports that they have netted more than 3 billion dollars thus far. From January 2015-June 2016, there was an increase of 1500% in successful attacks. That's one heck of a statistic. Basically, someone who has authority to order money wired appears to be e-mailing someone who actually does the wiring. Law firms have been hit hard by these scams, so it is critical that employees understand how they work and that they be conditioned to seek affirmation of any order to transfer significant monies.

More in the Morass

Clearly, there is a wealth of threats that employees need training on – more than we can possibly address in a single article. Employees need to be trained on the dangers of metadata, the safe use of public Wi-Fi, the safe use of file syncing software in the cloud, the perils of using social media, the need to protect all devices (including Apple devices), the malware that may be present on public computers in hotel business centers, public libraries and Internet cafés, the need to make sure (if they work from home without a VPN) to make sure that their home Wi-Fi is secure, how to secure their smartphones (especially if they are allowed to connect personal devices to the firm network), and the need for managed vendor access.

Hopefully, you have a sense of how critical it is that you train your law firm employees on cybersecurity. We know of one firm in California that averted disaster because all employees had recently received training on phishing e-mails and when they were on the receiving end of a targeted attack against their law firm, the employees recognized the phishing e-mails and quickly spread the word. Disaster averted. We have no doubt that the firm invested time and money in the training, but we're betting that, having survived the attack, the firm counted every dollar as well spent!

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

Secure Computing Abroad: Evolving Law Firm Policies

by Sharon D. Nelson, Esq. and John W. Simek

Traveling abroad? Worried about pickpockets? We have far bigger worries these days. If you travel abroad, you also have to worry about foreign governments – and our own – which may be interested in our data. Lawyers are not only not exempt from that interest – they are magnets. And when *The New York Times* published an article early this year about safeguarding data when crossing the border, we knew we were seeing a new hot cybersecurity topic – one that has primarily been considered at very large firms, until all the recent stories caught fire in the news. This article will focus on the dangers presented by our own government (the current runaway headline), but the advice is generally applicable to the risks presented by foreign governments, risks which may increase as there seems to be a worldwide ratcheting up of device seizure and examination at borders.

Three U.S. Border Incidents

There have been many, many border incidents, but here are three that caught our attention. A U.S.-born NASA scientist, Sidd Bikkannavar, returned to the U.S. in January of 2017. A seasoned international traveler, he flew back from Santiago, Chile to the George Bush Intercontinental Airport in Houston, Texas on Monday, January 30th, just over a week into the Trump administration.

Bikkannavar says he was detained by U.S. Customs and Border Patrol (CBP) and pressured to give the CBP agents his phone and access PIN. Since the phone was issued by NASA, it may have contained sensitive material that wasn't supposed to be shared. A Customs officer presented Bikkannavar with a document titled "Inspection of Electronic Devices" – which mentioned detention and seizure - and explained that CBP had authority to search his phone.

Bikkannavar was not allowed to leave until he gave CBP his PIN. Ultimately, feeling pressured, he agreed to hand over the phone and PIN. The officer left with the device and didn't return for another 30 minutes. The phone was returned to Bikkannavar, though he's not sure what happened during the time it was in the officer's possession. When it was returned, he immediately turned it off because he knew he had to take it straight to the IT department at NASA's Jet Propulsion Laboratory (JPL). The cybersecurity team at JPL was not happy about the breach.

Haisam Elsharkawi, an American citizen, was about to travel from Los Angeles to Saudi Arabia in February of 2017 when he was stopped at the airport, questioned, handcuffed, questioned some more and then released without charges three hours after his flight had departed. He reported that officers from the United States Customs and Border Protection repeatedly pressured him to unlock his cellphone so that they could scroll through his contacts, photos, apps and social media accounts. He said they threatened to seize the phone if he did not comply.

Also a veteran international traveler, he was appalled but felt pressured to unlock his phone and a Homeland Security agent looked through it for about 15 minutes.

In October of 2016, border agents seized phones from a Canadian photojournalist. He refused to unlock the phones, citing his obligation to protect his sources – he was blocked from entering the U.S.

As of March 13, 2017, NBC News had examined 25 cases in which American citizens said that CBP officials demanded that they hand over their phones and their passwords – or unlock them. In 23 of the 25 cases, these individuals were Muslim.

Keeping Private Data Private

Stories like these prompted *The New York Times* to investigate how to protect private data. As the paper states, U.S. citizens are not required to unlock their phones or share passwords with U.S. government officials. However, rules may vary depending on where you are traveling to and from. But being detained and intimidated is not an experience any traveler wants to go through.

So the *Times* recommended traveling with clean phones (so-called "burner" phones are often available at airports, as are phones you can rent) and clean tablets or laptops. It is recommended that you disable fingerprint readers because, in the U.S., law enforcement agencies can use warrants to compel you to unlock your phone with your fingerprint. We would go further and advise disabling all biometrics used to get into your phone, such as iris scans and facial recognition.

If you tell an official that you will not give up your password, the official may not be happy - to put it mildly. Better to use a password manager and tell the agent that you don't remember your one very long master password. And to avoid complications, don't have your password management software loaded on your devices. It is best to store the password vault (encrypted of course) in a cloud service like Dropbox and get access to it when you reach your destination.

If you are asked for passwords to your social media accounts or your e-mail, you can protect yourself by having two-factor authentication enabled – assuming that you have left your phone at home. Since the text code will be sent to that phone, officials will be unable to get into your accounts even with your password. You could leave your phone with someone you trust and get those codes that way but the general advice is to forego the use of social media while abroad.

When dealing with e-mail, do not install and configure any e-mail client on your laptop or cell phone. You don't want to have any e-mail on your devices. You should use some sort of remote access solution (e.g. Citrix, LogMeIn, etc.) to access your e-mail. Even using a browser could leave remnants of confidential information on your device.

Any device you use while abroad should be encrypted. The best way to ensure that your data remains secure is to back up your data to a cloud service and then wipe all of your devices before you return home. Once home, you can restore your data from the backup.

No matter what device you use abroad, assume that all electronic communication is subject to interception. This means you should always be using a secure encrypted connection. Make sure you have a properly configured VPN available and know how to use it.

The Authority of U.S. Customs and Border Protection Agents

Not only were we almost completely ignorant about the authority of CBP agents, it turns out that most lawyers have little knowledge of how expansive CBP authority really is. CPB officers have search power extending 100 air miles inland from any external boundary of the U.S. They can stop and question people at fixed checkpoints dozens of miles from U.S. borders. They can also pull over motorists whom they suspect of a crime as part of roving border patrol operations.

You might say - But doesn't the Fourth Amendment protect us from "unreasonable searches and seizures?" Yes – however, those protections are lessened when entering the country at international terminals at airports, other ports of entry and any location within 100 air miles of a U.S. boundary.

According to federal statutes, regulations and court decisions, CBP officers have the power to inspect, without a warrant, any person trying to gain entry into the country – and their belongings. The CBP's authority extends to examining computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players, and any other electronic or digital devices. That cuts a wide swath.

Current CBP policy dictates that officials should search electronic devices with a supervisor in the room when feasible and also in the presence of the person being questioned "unless there are national security, law enforcement or other operational considerations" that take priority. We already know that this language has been invoked to examine devices outside the presence of the person being questioned. CBP says it can conduct these searches "with or without" specific suspicion that the person possessing the items is involved in a crime.

With the approval of a supervisor, CBP officers can seize an electronic device – or a copy of the information on the device – "for a brief, reasonable period of time to perform a thorough border search." Typically, such seizures should be no more than five days (which seems a lot to us), but officers can apply for extensions in up to one-week increments. If the review of the device and its contents doesn't manifest probable cause for seizing it, CBP says it will destroy the copied information and return the device to the owner.

What if you are a lawyer? CBP has recognized that lawyers have an attorney-client privilege, but all this seems to mean is that agents have to get approval from an agency attorney before proceeding with the search. Not terribly comforting – and we suspect this is the reason why we have seen so many firms begin specifically to address the potential problems of re-entering the U.S.

What Have the Courts Said?

Unfortunately, the Supreme Court has not directly ruled on whether the CBP can search electronic devices without any specific suspicion that the owner might have committed a crime. In 2013, a decision for the U.S. Court of Appeals for the Ninth Circuit (http://cdn.ca9.uscourts.gov/datastore/opinions/2013/03/08/09-10139.pdf) affirmed that a cursory search of a laptop – for instance, having an owner turn on his/her devices and examining their contents – does not require any specific suspicions about the traveler. The court raised the bar for a "forensic

examination" of the devices such as using "computer software to analyze a hard drive." For these more comprehensive and intrusive searches, including password-protected information and other private data, officials must have a "reasonable suspicion" of criminal activity. That court decision applies only to the nine Western states in the Ninth Circuit.

We like this quote from the court's decision: ""Laptop computers, iPads and the like are simultaneously offices and personal diaries. They contain the most intimate details of our lives . . . It is little comfort to assume that the government — for now — does not have the time or resources to seize and search the millions of devices that accompany the millions of travelers who cross our borders. It is the potential unfettered dragnet effect that is troublesome."

During the 2016 fiscal year, CBP officials conducted 23,877 electronic media searches, five times as many as in 2015. That's a striking escalation.

What Law Firms Are Doing

As part of our research for this article, we were given access to one law firm's security precautions when traveling abroad. They included the following guidelines:

- Use one of the firm's "clean" loaner laptops, wiping the laptop before returning home
- Store all documents on the firm's network – store nothing on the laptop
- Use a burner phone (not a smart phone) for calls and texting.
- Access the firm's network via Citrix for e-mail and documents from the laptop - do not access the network from the phone.
- Do not use Bluetooth.
- Lock the laptop in the hotel room safe or in locked luggage.
- Make sure microphones and cameras are turned off.
- Change your network password before leaving the U.S., change it again once you return, after you have turned in your loaner laptop.

We have boiled the essential instructions down – as you can imagine, the instructions are far more detailed. A guiding principle is that authorities cannot search what you don't have. For those who want to chance it and have their device/data with them, make sure the device is encrypted and that it is powered down before going through Customs.

Several experts have published arcane methods of protecting your data, but we have not included them as being beyond the ken of most attorneys. And none of them will protect you from actually facing an angry CBP (or foreign) agent telling them that you really don't have any way to get to your data. We much prefer the "they can't search what you don't have" way of thinking.

In March of 2017, The Electronic Frontier Foundation published a fairly lengthy guide called "*Digital Privacy at the U.S. Border: Protecting the Data on Your Devices and in the Cloud*" which is worth reading and may be found at https://www.eff.org/wp/digital-privacy-us-border-2017.

Conclusion

In an article, it is impossible to examine every possible precaution that lawyers might use to protect client data while abroad. And though we've focused on the U.S. border because of current events, we have spent years watching videos of the Chinese spies accompanying maids to hotel rooms and inserting a flash drive in a businessman's computer. And we've heard stories from our large law firm friends of laptops coming back from abroad with "a little something extra" – that transmits data back "home". If you are a mid-to-large firm lawyer, your firm probably has very competent IT/cybersecurity help to assist you – don't be afraid to ask questions! And if you are a solo or small firm lawyer, make sure you engage someone who has both technical and security certifications to help you make sure you have the necessary security precautions in place.

The authors would like to thank their friend, journalist Ben Kerschberg, for his kind assistance in researching some aspects of this article.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, cybersecurity and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com

Can You Trust Your Expert Witnesses with Confidential Data?

by Sharon D. Nelson, Esq. and John W. Simek

Not always. There was a recent case in which confidential data was not, to put it mildly, well handled. The corporate defendant, a mortgage servicer, was accused of violating a consumer's privacy rights based on the manner in which it handled collection calls. The defendant protected its customer data with layers of network security consistent with best practices and ISO guidelines. During discovery, the plaintiff's experts received the calling data and copies of the customer service call recordings.

Both experts had unrelated full-time day jobs. Their expert witness work was a side business run out of their homes. Neither expert had a technical degree, and neither had taken a course in data security for over a decade. Both experts stored the sensitive case data in their homes. There were no locks on the doors to their home offices, so anyone in the houses had access to the drives. Neither expert was familiar with the basic ISO standards relating to data security. Neither had a written data security plan for their home network, and no outside company had ever performed vulnerability or penetration testing on their networks. One expert had no automatic intrusion detection software on his network. Both routinely produced data with sensitive PII (personally identifiable information) in unencrypted form.

The produced debt-collection calls included highly personal discussions in which debtors explained why a mortgage was in default, such as health or financial problems. One expert testified that he kept these recordings on an unencrypted portable laptop and accessed it on his home and public Wi-Fi networks. He also produced the call recordings to a third party to obtain technical assistance. The third party was not asked to execute the protective order, and that data presumably still resides on the third party's servers.

Well, you get the message. Expert witnesses, including us, routinely receive highly sensitive PII for review and analysis. Sensitive PII (SPII) is data that, if lost, compromised or disclosed without authorization, could result in substantial harm or embarrassment to the individual.

Attorneys cannot ignore how their experts manage the data produced to them. When highly sensitive data is produced in a lawsuit, it is removed from the protected network environment built by the data's owner and produced to the lawyers on the other side. The manner in which it is produced is up to the producing party. Sometimes the data is scrubbed of identifying information, such as names and dates of birth, but not always. Sometimes it is produced on encrypted drives, but again, not always. Instructions are rarely given to an expert regarding the manner in which to store the data or the type of security controls that need to be employed to keep it safe from unauthorized disclosure. That is certainly true. I can only recall a handful of cases where attorneys have given us explicit instructions.

Confidential data produced in a lawsuit is often subject to a protective order that contains generic language that the data will be kept confidential. Protective orders typically do not specify the security measures that the receiving party needs to have in place. The promise to keep the data protected is considered enough.

Under most protective orders, the receiving party has the right to produce the confidential information it receives to its experts in the case. Those experts are in turn required to sign the protective order and promise to protect the data. Again, the promise to keep the data protected is considered enough.

Experts at sophisticated firms generally have very competent IT and cybersecurity support. They could still be breached, but it is less likely than when engaging experts who are self-employed or who work in small firms with limited support.

Concrete suggestions?

Pay attention to physical security. Our forensics lab requires a prox card and a registered fingerprint to enter. Entries into or out of the lab are video recorded. There is a dual authenticated safe in the lab for high profile cases. Only three of us have access to that safe. We have a security system with motion sensors – and the police will be summoned unless someone with authority quickly acknowledges an equipment problem or a mistake (such as arming the system when someone is still in the lab – and yes, of course that has happened). We have a human receptionist monitoring the front door – in addition to more surveillance cameras. The building itself is locked nights and weekends.

Pay attention to logical security. Our evidence is on standalone offline hard drives or on a NAS unit which has no Internet access. The local network in the forensics lab is dedicated to forensic usage, unconnected to our corporate network. There are software and hardware protections for the lab network as well.

Pay attention to production security. It is the way of the world that most of our productions, by the instructions of our clients, are made via Dropbox. It makes sense since it is instantly available though one must trust that authorized access is not given by the receiving party to anyone who shouldn't have it. All production files are encrypted using 7-Zip before being placed in Dropbox with the password given via phone or a separate e-mail (not the e-mail containing the Dropbox link). If a file is not so large that it cannot be accommodated by Mimecast's Large File Send, we may use that – the data is encrypted as part of the process.

If we use the old school method of shipping drives, they are always encrypted.

There may be more security measures that are not coming to mind, but those are the basics. And, of course, if there is a court order with specific mandates, that order must be strictly adhered to. Most of them, as noted, do not require specifics measures.

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