Safeguarding Client Data: Attorneys' Legal and Ethical Duties

David G. Ries
Clark Hill PLC
412.394.7787
dries@clarkhill.com

April 2021

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.

Source: Shutterstock

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:[1]

> 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 paper is periodically updated and used as course materials for programs for the American Bar Association and other legal groups. Condensed versions of it have been published in articles including David G. Ries, "Cybersecurity for Attorneys: The Ethics of Incident Response," *Law Practice Today* (November 2020), David G. Ries, "Cybersecurity for Attorneys: Addressing the Legal and Ethical Duties," *Law Practice Today* (November 2019), David G. Ries, "Safeguarding Client Data: Legal Ethics in a Breach-a-Day World," *Trusts & Estates* (February 2018) and David G. Ries, "Cybersecurity for Attorneys: Understanding the Ethical Obligations," *Law Practice Today* (March 2012).

© 2012-2021 David G. Ries. All rights reserved. Revised 4-6-2021.

This is true today for attorneys and law firms as well as other businesses and enterprises. American Bar Association (ABA) Formal Opinion 477R (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 Cybersecurity Legal Task Force serves as a clearinghouse regarding cybersecurity, including information on threats.[2] During 2018, The *ABA Journal* and the Task Force jointly produced a series of articles, "Digital Dangers – Cybersecurity and the law" that provide a variety of information on digital threats to attorneys and ways of addressing them.[3]

The Introduction to ABA Formal Opinion 483 (October 2018) (discussed below) includes:

> Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession. As custodians of highly sensitive information, law firms are inviting targets for hackers. In one highly publicized incident, hackers infiltrated the computer networks at some of the country's most well-known law firms, likely looking for confidential information to exploit through insider trading schemes. Indeed, the data security threat is so high that law enforcement officials regularly divide business entities into two categories: those that have been hacked and those that will be.

Law.com published a series of articles on law firm data breaches in October of 2019. It reported on over 100 breaches, based on its review of state websites and information requests to states about breaches reported to states by law firms under data breach notice laws. The first article started with: [4]

> A Law.com investigation finds that law firms are falling victim to data breaches at an alarming rate, exposing sensitive client and attorney information. These incidents—most unpublicized before now—may just be the tip of the iceberg.

The ABA's *2020 Legal Technology Survey Report* reports that law firms have been and continue to be victims of data breaches.[5] The *Survey* reports that about 29% 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 is "ever." A breach broadly includes incidents like a lost/stolen computer or smartphone, hacker, break-in, or website exploit. This compares with 26% in 2019 and 23% in 2018.

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. Threats from compromised third-parties, like service providers, are also a growing threat.

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.

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[6] 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), supervision (Model Rules 5.1, 5.2 and 5.3), and safeguarding property (Model Rule 1.15).

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 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 2021, 39 states have adopted this addition to the comment to Model Rule 1.1, some with variations from the ABA language.[7]

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" about use of technology. It requires notice to a client of a material 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:

> <u>(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.</u>

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, cybercriminals, 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. 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.

"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.

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.[8]

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 "Assist<u>ance</u>," 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.

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.

In June 2012, while the Ethics 20/20 amendments were under consideration, the *Wall Street Journal* published "Client Secrets at Risk as Hackers Target Law Firms."[9] It started with:

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

Ethics Opinions. A number of 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).[10] 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."

Another opinion on safeguarding client data is ABA Formal Opinion 477R, "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.

The next year, the ABA issued Formal Opinion 483, "Lawyers' Obligations After an Electronic Data Breach or Cyberattack" (October 2018). This opinion reviews lawyers' duties of competence, confidentiality, communication, and supervision in safeguarding confidential data and in responding to data breaches. It discusses the obligations to monitor for a data breach, stop a breach, restore systems, and determine 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 opinion notes that the ethical duty to notify applies to current clients. Applying Model Rule 1.9(c), it finds that there is not a requirement to notify a former client of a breach "as a matter of legal ethics."

In April of 2019, the Maine Professional Ethics Commission issued Opinion #220. "Cyberattack and Data Breach: The Ethics of Prevention and Response" (April 2019). Its conclusions under the Maine Rules of Professional Conduct are that same as ABA Formal Opinion 483, with the exception that it concludes that the duty to notify applies to both current and former clients.

State Bar of Michigan Opinion RI-381 (February 2020), "Duty to Understand Technology, Including Cybersecurity," provides an overview of attorneys' cybersecurity obligations, consistent with the opinions above. On breach notification, it states:

> A lawyer has a duty to inform a client of a material data breach in a timely manner. See MRPC 1.3 (duty to act with reasonable diligence and promptness in representing a client.) A data breach is "material" if it involves the unauthorized access, destruction, corruption, or ransoming of client ESI protected by MRPC 1.6 or other applicable law, or materially impairs the lawyer's ability to perform the legal services for which the lawyer has been hired. The duty to inform includes the extent of the breach and the efforts made and to be made by the lawyer to limit the breach.

The Pennsylvania Bar Association issued Formal Opinion 2020-300, "Ethical Obligations for Lawyers' Working Remotely" (April 2020) to address work-at-home issues arising from the COVID-19 pandemic. The opinion reviews attorneys' ethical duties to employ competent and reasonable measures to safeguard information relating to clients and provides best practices for attorneys performing legal work and communications remotely.

The opinion concludes:

> The COVID-19 pandemic has caused unprecedented disruption for attorneys and law firms and has renewed the focus on what constitutes competent legal representation during a time when attorneys do not have access to their physical offices. In particular, working from home has become the new normal, forcing law offices to transform themselves into a remote workforce overnight. As a result, attorneys must be particularly cognizant of how they and their staff work remotely, how they access data, and how they prevent computer viruses and other cybersecurity risks.
>
> In addition, lawyers working remotely must consider the security and confidentiality of their procedures and systems. This obligation includes protecting computer systems and physical files and ensuring that the confidentiality of client telephone and other conversations and communications remain protected.
>
> Although the pandemic created an unprecedented situation, the guidance provided applies equally to attorneys or persons performing client legal work on behalf of attorneys when the work is performed at home or at other locations outside of outside of their physical offices, including when performed at virtual law offices.

California Formal Opinion No. 2020-203 (unauthorized access by third parties to electronically stored confidential client information), consistent with the other opinions, covers attorneys' duty to assess risks and take reasonable steps to minimize risks. It also provides that attorneys are required to monitor for breaches, conduct a reasonable inquiry in the event of a breach, and to notify clients. It notes the difference between ABA Formal Opinion 483 and Maine Opinion #220 on duty to notify former clients but does not express a view on notice to former clients. Its Digest states:

> Lawyers who use electronic devices which contain confidential client information must assess the risks of keeping such data on electronic devices and computers, and take reasonable steps to secure their electronic systems to minimize the risk of unauthorized access. In the event of a breach, lawyers have an obligation to conduct a reasonable inquiry to determine the extent and consequences of the breach and to notify any client whose interests have a reasonable possibility of being negatively impacted by the breach.

Most recently, the ABA issued Formal Opinion 498, "Virtual Practice" (February 2021). Consistent with earlier ABA and state ethics opinions, its headnote includes:

> *…When practicing virtually, lawyers must particularly consider ethical duties regarding competence, diligence, and communication, especially when using technology. In compliance with the duty of confidentiality, lawyers must make reasonable efforts to prevent inadvertent or unauthorized disclosures of information relating to the representation and take reasonable precautions when transmitting such information. Additionally, the duty of supervision requires that lawyers make reasonable efforts to ensure compliance by subordinate lawyers and nonlawyer assistants with the Rules of Professional Conduct, specifically regarding virtual practice policies.*

The opinion includes a discussion of: 1. Hardware/Software Systems, 2. Accessing Client Files and Data, 3. Virtual meeting platforms and videoconferencing, 5. Virtual Document and Data Exchange Platforms, and 6. Smart Speakers, Virtual Assistants, and Other Listening-Enabled Devices.

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.[11] A June 2014 post by Google on the *Google Official Blog*[12] and a July 2014 *New*

"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

York Times article[13] 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[14] 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.[15] 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."[16] 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."[17]

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

In May 2017, the ABA Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 477R, "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 finds that "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 477R, 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 competent and reasonable efforts.

It explains that a:

> …lawyer has a variety of options to safeguard communications including, for example, using secure internet access methods to communicate, access and store client information (such as through secure Wi-Fi, the use of a Virtual Private Network, or another secure internet portal), using unique complex passwords, changed periodically, implementing firewalls and anti-Malware/Anti-Spyware/Antivirus software on all devices upon which client confidential information is transmitted or stored, and applying all necessary security patches and updates to operational and communications software." Furthermore, "[o]ther available tools include encryption of data that is physically stored on a device and multi-factor authentication to access firm systems.

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.

Pennsylvania Formal Opinion 2020-300, "Ethical Obligations for Lawyers' Working Remotely" (April 2020) (discussed above), referencing ABA Formal Opinion 477R, provides an overview of attorneys' obligations to protect electronic communications, including the use of encryption when appropriate.

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.

Conclusion – Ethics Duties

The key professional responsibility requirements from these ethics rules and opinions are: (1) competent and reasonable measures to safeguard client data, including electronic communications, (2) communication with clients, (3) appropriate supervision, and (4) ongoing review as technology, threats, and available safeguards evolve. Competence requires an understanding of limitations in attorneys' knowledge and obtaining appropriate assistance when necessary. Communication includes obtaining clients' informed consent, in some circumstances, and notifying clients of a material breach or compromise. It is important for attorneys to consult the rules, comments, and ethics opinions in the relevant jurisdiction(s).

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.[18]

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.[19]

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, 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."[20] 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 Information Technology staff 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:[21]

> 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.)

At the ABA Annual Meeting in August 2014, the ABA adopted a resolution on cybersecurity that is consistent with this general approach:[22]

> **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.

An initial 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 and data 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.

Cybersecurity is best viewed as a part of the information governance process, which manages documents and data from creation to final disposition – including security and privacy.[23] Managing data is a critical part of information governance, including security, privacy, and records and information management. Effective management includes a current inventory, classification, safeguarding, managing from creation to final disposition, and secure disposition where appropriate. Effective management requires minimization of data – collection and retention of only what is necessary and secure disposition of data that is no longer required or needed. **Management and minimization of data is an essential part of an effective security program.**

A cybersecurity 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.[24] Since it is now into 2021, it will be interesting to see the actual current percentages.

An incident response plan is an important part of a cybersecurity program. Like the program, the plan should be appropriately scaled to the size of the firm and the sensitivity of the information. Identifying internal and external resources and preparing processes and technology in advance is necessary for effective incident response.[25]

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."

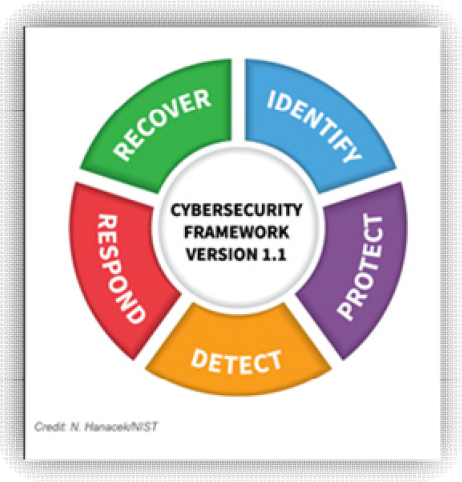
Security involves thorough analysis and often requires balancing and trade-offs to determine what risks and safeguards are reasonable under the circumstances. There is frequently a trade-off between security and usability. Strong security often makes technology very difficult to use, while easy to use 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 cybersecurity.

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),[26] other more comprehensive NIST standards, like NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations* (September 2020)[27] 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,[28] (consensus international standards for comprehensive Information Security Management Systems (ISMS) and elements of them). The Center for Internet Security has published the *CIS Controls* v7.1[29] that provide globally recognized best practices for securing IT systems and data.



Source: NIST

These standards can be a challenge for small and mid-size firms. In October of 2018, the Federal Trade Commission (FTC) launched a new website, Cybersecurity for Small Business, which includes links to a number of security resources that are tailored to small businesses.[30] 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*.[31] In March of 2019, NIST launched its Small Business Cybersecurity Corner website.[32]

The ABA Cybersecurity Legal Task Force maintains a web page that includes resources for attorneys and law firms generally and for solo practitioners and small law firms.[33]

The ABA now offers as a member benefit a variety of free live and on demand webinars, including a number of webinars on cybersecurity and privacy. They're a great resource – and free for members.[34] Recent examples include: "Security Assessments and Pen Testing for Law Firms" (April 14, 2021 and on demand),[35] "Ransomware 101 for Lawyers: Protection, Response and Recovery" (September 17, 2020 and on demand),[36] "Working Remotely: Ethical Considerations During and After COVID-19" (May 14, 2020 and on demand,)[37] and "Best of ABA TECHSHOW: Anatomy of a Data Breach: Analyzing Past Breaches to Minimize Risk" (February 4, 2020 and on demand).[38]

ILTA (the International Legal Technology Association) has a LegalSEC initiative that provides the legal community with guidelines for risk-based information security programs, including publications, 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.[39]

The Sedona Conference, a research and educational institute, has published *The Sedona Conference Commentary on Law Firm Data Security* (July 2020).[40] It identifies "ways that organizations and their law firms should approach and address organization expectations and firm capabilities regarding data security."

Law firms and other businesses and organizations are currently facing security challenges from the COVID-19 shut-downs and expanded remote access and work-at home. Government agencies and security organizations have recently provided updated standards and guidance to address these remote work challenges. Examples include the Cybersecurity and Infrastructure Security Agency (CISA),[41] NIST,[42] the National Security Agency (NSA),[43] the Center for Internet Security (CIS),[44] and the SANS Institute.[45] As with the standards and frameworks, it is best to review these resources, select one or more that best fit a law firm's circumstances, and use it or them in the security process.

Source: Shutterstock

A comprehensive cybersecurity program should include the following elements. While checklists are helpful for cybersecurity programs, it important to use them appropriately. Security is not a "check the box" or "set it and forget it" process. It is important to devote continuing attention to security and to periodically review and update cybersecurity programs.

- **Assignment of responsibility for security,**
- **Managing and minimizing data,**
- **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 reviews and audits 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 (MSSP) 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.

Secure cloud services, like Microsoft 365 (Office 365), Google Work (G Suite), and cloud practice management platforms, can provide a higher level of security than many attorneys and law firms can provide on their own, particularly for solos and small and mid-size firms. In selecting and using cloud services, attorneys should follow the recommendations in the cloud ethics opinions discussed above, including "reasonable care to ensure that confidentiality is maintained in a manner consistent with the lawyer's obligations under Rule 1.6." It is important to securely configure the cloud service (like using multifactor authentication and enabling and retaining logs), to provide for security of the endpoint computers and devices connecting to the cloud, and to provide a secure connection to the cloud (like a virtual private network). Managing third-party

security risks is important for all service providers and others that can connect to a law firm network.

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. It is important to consult with an attorney or broker with current experience in this area.

The ABA Center for Professional Responsibility has published *Protecting Against Cyber Threats: A Lawyer's Guide to Choosing a Cyber Liability Insurance Policy, Second Ed.* (2020) that provides guidance in this area.[46] The ABA recently presented a webinar on this topic, "Best Practices for Placing Cutting Edge "Cyber" Insurance: Policyholder, Insurer and Broker Perspectives" (August 20, 2020 and on demand).[47]

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 addressing 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

American Bar Association, Business Law Section, Cyberspace Law Committee, www.americanbar.org/groups/business_law/committees/cyberspace

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

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

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

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

American Bar Association, Section of Science and Technology Law, Information Security Committee, www.americanbar.org/groups/science_technology/committees

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

Cybersecurity and Infrastructure Security Agency (CISA), 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)

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, 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)** (Third Edition planned for late 2021 or early 2022)

The Sedona Conference*, The Sedona Conference Commentary on Law Firm Data Security* (July 2020), https://thesedonaconference.org/publication/Commentary_on_Law_Firm_Data_Security.

David G. Ries is of counsel in the Pittsburgh, PA office of Clark Hill PLC, where he practices in the areas of technology, data protection, and environmental law and litigation. For over 25 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.* (American Bar Association 2016) and *Encryption Made Simple for Lawyers* (American Bar Association 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 Cross-Sector Council, and ILTA's LegalSEC.

Endnotes

[1] 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.

[2] ABA Legal Task Force home page, www.americanbar.org/groups/cybersecurity.

[3] Summaries of the articles and links to them are available at www.abajournal.com/magazine/cyber.

[4] Christine Simmons**,** Xiumei Dong and Ben Hancock**,** "More Than 100 Law Firms Have Reported Data Breaches. And the Problem Is Getting Worse," Law.com (October 15, 2019), www.law.com/2019/10/15/more-than-100-law-firms-have-reported-data-breaches-and-the-picture-is-getting-worse. See also, Christine Simmons**,** Xiumei Dong and Ben Hancock**, "**Law Firm Cybersecurity: See Which Firms Reported a Data Breach," Law.com (October 15, 2019), www.law.com/2019/10/15/here-are-law-firms-reporting-data-breaches, Christine Simmons**,** Xiumei Dong and Ben Hancock**,** "How Vendor Data Breaches Are Putting Law Firms at Risk," Law.com (October 17, 2019), www.law.com/2019/10/17/how-vendor-data-breaches-are-putting-law-firms-at-risk and Christine Simmons and Xiumei Dong, "As Hackers Get Smarter, Can Law Firms Keep Up?" Law.com (October 28, 2019), www.law.com/2019/10/28/as-hackers-get-smarter-can-law-firms-keep-up.

[5] See, John G. Loughnane, *ABA TECHREPORT 2020 Cybersecurity*, www.americanbar.org/groups/law_practice/publications/techreport/2020/cybersecurity.

[6] ABA Model Rules of Professional Conduct (2021) (Model Rules).

[7] LawSites Blog, "Tech Competence," www.lawsitesblog.com/tech-competence.

[8] "The proposed amendment [to Model Rule 1.1], which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent. … This duty is already described in several existing Comments, but the Commission concluded that, in light of the pervasive use of technology to store and transmit confidential client information, this existing obligation should be stated explicitly in the black letter of Model Rule 1.6." ABA Commission on Ethics 20/20, *Report to Resolution 105A Revised*, (2012).

[9] Jennifer Smith, "Client Secrets at Risk as Hackers Target Law Firms," *Wall Street Journal Law Blog* (June 25, 2012), https://blogs.wsj.com/law/2012/06/25/dont-click-on-that-link-client-secrets-at-risk-as-hackers-target-law-firms.

[10]The ABA Legal Technology Resource Center has published a summary with links, "Cloud Ethics Opinions around the U.S.," available at www.americanbar.org/content/dam/aba/images/legal_technology_resources/CloudEthicsOpinions2019/cloudethicsopinions2019.pdf.

[11] 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).

[12]"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.

[13] 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.

[14] 18 U.S.C. §§ 2510-2522.

[15] 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.").

[16] File password protection in some software, like current versions of Microsoft Office, Adobe Acrobat, and WinZip uses encryption to protect security. Adobe Acrobat also containers for multiple files called PDF Portfolios that can be encrypted with password protection. They are sometimes easier to use than encryption of e-mail and attachments. However, the protection can be limited by use of weak passwords that can be easy to break or "crack."

[17] Peter Geraghty and Susan Michmerhuizen, "Encryption Conniption," *Eye on Ethics, Your ABA* (July 2015.

[18] www.acc.com/resource-library/model-information-protection-and-security-controls-outside-counsel-possessing-0.

[19] 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).

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

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

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

[23] See the Information Governance Reference Model (IGRM), published by EDRM, an organization that publishes resources for e-discovery and information governance (www.edrm.net/frameworks-and-standards/information-governance-reference-model) and ARMA International, Information Governance (www.arma.org/page/Information_Governance).

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

[25] See Sharon D. Nelson, David G. Ries, and John W. Simek, "What to Do *When* Your Data is Breached," *Michigan Bar Journal* (September 2018), David G. Ries, "Cybersecurity for Attorneys: The Ethics of Incident Response," *Law Practice Today* (November 2020) and *The Sedona Conference Incident Response Guide* (January 2020), www.michbar.org/file/barjournal/article/documents/pdf4article3480.pdf, www.lawpracticetoday.org/article/cybersecurity-attorneys-ethics-incident-response and https://thesedonaconference.org/publication/Incident_Response_Guide.

[26] www.nist.gov/cyberframework.

[27] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

[28] www.iso.org/isoiec-27001-information-security.html.

[29] www.cisecurity.org/controls.

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

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

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

[33] www.americanbar.org/groups/cybersecurity/small-solo-resources/aba-cybersecurity-resources-for-small-solo-law-firms.

[34] www.americanbar.org/cle-marketplace/cle-library.

[35] www.americanbar.org/events-cle/mtg/web/411370011.

[36] www.americanbar.org/events-cle/ecd/ondemand/403496872.

[37] www.americanbar.org/events-cle/mtg/web/399544145.

[38] www.americanbar.org/events-cle/ecd/ondemand/392937589.

[39] www.iltanet.org/resources/legalsec?ssopc=1.

[40] https://thesedonaconference.org/publication/Commentary_on_Law_Firm_Data_Security.

[41] www.cisa.gov/telework.

[42] www.nist.gov/blogs/cybersecurity-insights/telework-security-basics.

[43] www.nsa.gov/News-Features/News-Stories/Article-View/Article/2163484/working-from-home-select-and-use-collaboration-services-more-securely.

[44] www.cisecurity.org/white-papers/cis-controls-telework-and-small-office-network-security-guide.

[45] www.sans.org/security-awareness-training/sans-security-awareness-work-home-deployment-kit.

[46] www.americanbar.org/products/inv/book/385016340.

[47] www.americanbar.org/events-cle/ecd/ondemand/402271438.

Attachment 1: Cybersecurity Program Checklist

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

A comprehensive cybersecurity program should include the following elements. While checklists are helpful for cybersecurity programs, it important to use them appropriately. Security is not a "check the box" or "set it and forget it" process. It is important to devote continuing attention to security and to periodically review and update cybersecurity programs.

- ☐ **Assignment of responsibility for security,**
- ☐ **Managing and minimizing data,**
- ☐ **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.**

Provided by:
David. G. Ries
Clark Hill PLC
Pittsburgh, PA
dries@clark hill.com
412.394.7787

Attachment 2: Practical Security Checklist

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

This checklist supplements the Comprehensive Cybersecurity Program Checklist and covers practical measures to implement a cybersecurity program. While checklists are helpful for cybersecurity programs, it important to use them appropriately. Security is not a "check the box" or "set it and forget it" process. It is important to devote continuing attention to security and to periodically review and update cybersecurity programs.

- ☐ **Use secure, common configurations for servers, desktops, laptops, and mobile devices.**
    - This includes settings like automatic logoff or shut down after *x* minutes of inactivity and locking or wiping after *x* failed logon attempts.
    - Follow security configuration recommendations from Microsoft, Apple and device manufactures.
    - For more comprehensive recommendations, see the Center for Internet Security's CIS Benchmarks, www.cisecurity.org/cis- benchmarks.
    - Most attorneys will need technical assistance with secure configuration of servers.
- ☐ **Control use of administrative privileges.**
    - Windows and Mac computers have two kinds of user accounts: administrator and standard user accounts.
    - Administrator access is needed for some functions like installing or removing software and devices.
    - Some malware can run only in an administrator account.
    - Use a standard user account for regular use of a computer.
- ☐ **Use strong passwords or passphrases and a password manager.**
- ☐ **Use multifactor authentication, particularly for administrator accounts and remote access.**
- ☐ **Segment networks and limit access to sensitive data.**

- **Promptly patch the operating system, firmware, all applications, and all plug-ins.**
    - Malware often takes advantage of vulnerabilities in operating systems, applications and plug-ins. Updates and patches are developed to protect against such vulnerabilities after they are known.
    - Patches should be promptly applied to protect against vulnerabilities.
    - Computers are often compromised by malware for which patches are available but have not been applied.
- **Provide for secure electronic communications.**
    - It has now reached the point where attorneys should have access to encrypted e-mail for use when appropriate.
    - There are now multiple options for encrypted e-mail that are inexpensive and easy to use.
    - Examples include business versions of Microsoft 365 (Office 365) and Google's G Suite and services like ZixMail and Citrix FileShare.
- **Use strong encryption.**
    - Business versions of Windows have built-in encryption called BitLocker. It is activated by turning it on and saving a recovery key. BitLocker works best on business grade desktops and laptops that have a TPM (Trusted Platform Module) security chip. For consumer versions of Windows, encryption software is available from the publishers of standard security software like Symantec, McAfee, Norton and Sophos. Standalone encryption software is available from providers like Dell and WinMagic.
    - Apple computers have built-in encryption called FileVault (currently FileVault 2). It is activated by turning it on and saving a recovery key.
    - iPhones and iPads have built-in encryption that is automatically enabled when a passcode is set.
    - Newer Android devices work the same way as iPhones and iPads, with encryption automatically enabled when a PIN, passcode, or swipe pattern is set.
    - Older Android devices require encryption to be enabled by checking a box or pressing an onscreen button. If you are enabling encryption on an Android device that is already in use, follow the onscreen instructions, including plugging the device into a charger.
    - After encryption is enabled, the device is automatically encrypted when a user logs off or the device is shut down. It is automatically decrypted when a user enters his or her logon credentials.

- **Use only secure wireless networks.**
    - Securely configure law office wireless networks and home wireless networks used for work and use only ones with WPA2 or WPA3 security. Do not use wireless clouds with outdated WEP or WPA security.
    - Do not use public wireless networks unless you confirm that you have a secure connection by using a VPN (Virtual Private Network) or other secure communication channel.
- **Use strong security appliances and software and keep them up to date.**
- **Use email filtering and website filtering.**
- **Conduct vulnerability assessment and remediation.**
- **Back up important files and data.**
    - Files should be backed up at least daily.
    - Backups should be configured in a way that they won't be immediately compromised by malware that impacts the operating computer or network. This is particularly important for ransomware.
    - Test backups.
- **Address third party security risks.**
    - It's important to conduct due diligence to determine that the level of security and the terms of service are appropriate.
    - Attorneys should require by contract that the services will be provided in a way that is consistent with the attorney's ethical duties, particularly confidentiality.
    - Attorneys should also engage in appropriate monitoring or supervision.
- **Consider using secure cloud service providers.**
    - Service providers like business and enterprise versions of Microsoft Office 365 and Google's G Suite and secure case management platforms can generally provide a higher level of security than all but very large law firms.
    - Business versions of services like Dropbox and Box provide stronger control and security than consumer versions.
    - It's important to conduct due diligence to determine that the level of security and the terms of service are appropriate.
- **Provide for secure disposal of electronic data and paper.**
    - Paper records should be shredded or incinerated.
    - Electronic data should be wiped or deleted with secure deletion software.

- Devices that can’t be securely wiped with software should be physically destroyed.

- **Address security for new, current, and departing employees.**

Attachment 3: Common Secure Configuration Checklist

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

This checklist provides more details for implementing one of the measures in the Practical Security Checklist. While checklists are helpful for cybersecurity programs, it important to use them appropriately. Security is not a "check the box" or "set it and forget it" process. It is important to devote continuing attention to security and to periodically review and update cybersecurity programs.

- ❑ **Follow set up instructions for operating system and device**
- ❑ **Set up administrator and standard user accounts**
- ❑ **Use a strong pass word / passphrase**
- ❑ **Set up auto lock after *x* mins of inactivity**
- ❑ **Set up lock after x incorrect log on attempts**
- ❑ **Enable encryption (+ save recovery key)**
- ❑ **Turn on firewall**
- ❑ **Use current operating system and apps**
  - with all current updates (auto update where available)
- ❑ **Install security software (auto update)**
- ❑ **Secure Internet browser**
- ❑ **Turn off unneeded services**

More details are available in:

- NIST's, National Checklists Program, https://nvd.nist.gov/ncp/repository, and
- The Center for Internet Security's CIS Benchmarks, www.cisecurity.org/cis- benchmarks, and
- Microsoft's Security Baselines, https://techcommunity.microsoft.com/t5/microsoft-security-baselines/bg-p/Microsoft-Security-Baselines.

Attachment 4: An Encryption Quick Start Action Plan

[This Action Plan is from Sharon D. Nelson, David G. Ries and John W. Simek, *Encryption Made Simple for Lawyers* (American Bar Association 2015). References are to Chapters in the book.]

An American Bar Association resolution adopted in August 2014 *"encourages private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected*." It covers attorneys and law firms, as well as other businesses and enterprises. An appropriate information security or cybersecurity program is an essential part of compliance with attorneys' duty under ABA Model Rule 1.6(c) to employ "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Encryption of data is a critical component of an appropriate information security or cybersecurity program. (Chapters 2 and 3)

This Quick Start Action Plan outlines the steps that attorneys can take to implement encryption – **starting now**.

1. **Start with the basics for encryption that you are using now or implementing in the future.** (Chapter 5)
    a. **If you need help in implementing encryption, find someone who is qualified to assist you.**
    b. **Protect encrypted data with strong authentication.**
    In many implementations of encryption, access to the decryption key is protected by the user's password or passphrase. Make sure that you have strong passwords or passphrases for encryption you are currently using or you plan to implement in the future.
    c. **Back up data.**
    Like other areas of technology, there can be technical failures with encryption hardware and software. Keep a secure backup of encrypted data, a step that should always be done, even for data that is not encrypted.
    d. **Back up the recovery keys.**
    In some implementations of encryption, a user can back up a recovery key that may make encrypted data recoverable if a user forgets a password or there is a technology problem. Back up the recovery key in a secure place. In mid-sized and larger firms, recovery keys should be managed by IT staff.
2. **Start with the "no-brainer" encryption solutions – encryption of laptops, smartphones, tablets, and portable drives.** (Chapters 5, 6 and 7)
    The Verizon 2014 Data Breach Investigation Report notes that "encryption is as close to a no-brainer solution as it gets" to protect confidential data on lost or stolen laptops and mobile devices. It's not just Verizon, this view is widely held by information security professionals and

government agencies. Review the devices that you and your firm are using – laptops, smartphones, tablets, and portable drives - and make plans to encrypt them as soon as reasonably possible if they are not already encrypted. With many of them, it's just a matter of turning encryption on. Consider encryption and enable it when you add new devices.

3. **Protect confidential documents with encryption – a solution you already have.** (Chapter 11) Confidential documents transmitted electronically or by e-mail should be protected by encryption. Current versions of Microsoft Office, Adobe Acrobat and WinZip encrypt documents when password protection is used. New Jersey Ethics Opinion 701 (April 2006 - over eight years ago) advised attorneys to password protect documents [encrypt them] when they are sent over the Internet. (Chapter 2.) While this form of encryption may not be as secure as some of the other solutions discussed in the book, it is much more secure than no encryption and is immediately available to most attorneys.

4. **Use secure network connections.** (Chapter 8)
Confidential data that is transmitted outside of a secure network should be protected. This requires secure connections between networks and over the Internet. Review the various network connections that you and your firm use and make sure that they are secure. For the Internet, you should use https:// or virtual private networks as a minimum.

5. **Secure your wireless networks.** (Chapter 8.)
Make sure that your law office wireless network and home networks used for client data are protected by WPA2 (Wi-Fi Protected Access 2) [or WPA3] encryption and are securely configured. If you are using an older wireless access device that does not support WPA2, replace it.

6. **Be careful on public networks.** (Chapter 8)
Make sure that you can use a public network securely for confidential data **before** you use it, or avoid using it. Use only secure connections – https:// or a virtual private network.

7. **Implement an encrypted e-mail solution.** (Chapter 9)
It has now reached the point where most or all attorneys should have the ability to use encrypted e-mail, where appropriate, for confidential communications. A basic level of protection can be provided by putting the confidential communication in a password protected/encrypted attachment. There are now a number of easy to use, inexpensive options that are available for securing e-mail, including ones for solos and small firms.

8. **Use encryption in the cloud.** (Chapter 10)
Encryption controlled by the end-user should be the default for confidential data stored in the cloud. End-user controlled encryption should be required for attorneys unless the attorney makes an informed decision that the data is not sensitive enough to require this level of protection or that the cloud service provider will implement and maintain sufficient security controls without end-user controlled encryption. For attorneys, this requires the analysis required by the ethics rules and opinions discussed in Chapter 2, including competent and reasonable measures to safeguard information relating to clients, due diligence concerning service providers, and requiring service providers to safeguard data in accordance with attorneys' confidentiality obligations.