Chapter 9

Small Firms and Sole Practitioners

Melissa Ventrone

I can hear some lawyers saying it now: "I'm just a solo. I don't need a complicated computer security system. I'm not at risk of a cyberattack. Besides, I don't have an IT department to handle it or a big budget to spend on computer security. I'm not as important as a large firm; no one would want to attack me."

Wrong. Solo practitioners and small firms are, in some instances, at higher risk of suffering a catastrophic cyberattack. These types of firms have smaller IT budgets and fewer resources to identify and address cybersecurity risks, meaning that a cyberattack can cause more damage to a small firm than it would a larger firm. Most attacks are not targeted at a particular company or individual. Instead, attackers conduct automated scans and attacks that search for and identify vulnerabilities in systems, which they then use to access the victim's system and perpetrate an attack.

First, while there is no guarantee that any cybersecurity system will be bulletproof, confidential client information can be lost if a casual approach to security is employed. Firms must take the appropriate steps to protect their systems and client information.

Second, the traditional requirement to protect the confidentiality of client information and work product[1] has been updated. State bar authorities

1 Model Rules of Pro. Conduct r 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" Comment [18] "The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, 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

in many states now require attorneys to be familiar with technology,[2] and employ reasonable technological safeguards as part of any attorney's commitment to be competent in the practice of law.[3]

Third, while you may think your firm is too small to be of interest to anybody, that is certainly not the case. Your client information may be significant to a competitor, a foreign government, a personal enemy, or a cybercriminal looking for a chance to make some money. Is there technology that might be cutting edge? Do you have clients with public profiles that might generate someone who wants to get revenge? Are your clients involved in negotiations to buy or sell a business where having inside information may be useful in stock trading? Someone might want to learn private information just for "doxing"—publishing private information on the Internet.

Fourth, if an attacker is able to disrupt your systems and prevent you from accessing data or programs, this will have a significant impact on your ability to provide services to your clients or meet key deadlines. If you cannot access e-mail, your document management system, or data on your laptop because an attacker has blocked access or encrypted all of your systems, your ability to provide services to your clients will be significantly impacted and may cause you to lose clients. It will certainly have a significant financial impact on your firm.

Fifth, and perhaps most importantly for solos and small firms, the failure to provide adequate security for the electronic aspects of your practice goes to the heart of your practice model. Technology allows solos and small firms to compete with bigger firms. Whether it is the ability to work from any location, to access huge stores of information, or to operate without

or important piece of software excessively difficult to use)." Any client whose data is lost due to a cybersecurity incident should be notified, but in most cases (e.g., not involving public companies or consumer personally identifiable information) small firms or solos probably will not be required to make public announcements of a security breach.

2. As of Feb. 1, 2021, 35 states had adopted this requirement.

3. Model Rules of Pro. Conduct r. 1.1: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." Comment [8]: "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject" (emphasis added).

big dedicated office server and staff, modern tools allow for the practice of law at the highest level of quality. You can compete with the big guys in many areas, and perhaps surpass their service levels with individual attention to clients, responsiveness, and transparent billing practices. But in order to compete you need to be able to provide your clients with the assurance that they will not be putting their data, their business, or even their lives, at risk. Some clients, particularly large companies, may well require a security audit before retaining your firm.

Cyberattacks are becoming more pervasive and destructive. As fast as we develop new ways to protect our systems, the cybercriminals find ways to bypass the protections and perpetrate the attack. For instance, ransomware attacks originally involved the attacker deploying malware that encrypted the data in the system. For a "fee" or "ransom," the attackers would provide a decryption key that the company could use to decrypt and recover its data. More companies started to use backups so they could quickly restore their systems if they suffered a ransomware attack. Now, an attacker steals data from its victim and will release the data publicly if the company does not pay the ransom. The cost to a small firm from the type of system interruption a ransomware attack would cause, coupled with the impact to its reputation if data is released, could be catastrophic.

It isn't a question of if you will experience a cyberattack; the appropriate questions are when, and are you ready? In addition to taking steps to protect your systems, you should also ensure you have implemented the following controls to enable you to recover quickly should an attack occur. They don't necessarily need to be done in the order they are listed here, but they should be done sooner or later—preferably sooner.

1. **Multifactor authentication.** Multifactor authentication (MFA) is one of the most important security controls small firms should implement for remote access to any system. MFA is the process of using two or more credentials to authenticate to a system. If a vendor or business partner needs access to your systems, you should require that they use MFA to do so. If you have services that are hosted, such as bank accounts, human resources, or cloud-hosted backup services, you should make sure access to any of these services is also protected by MFA. Access

to e-mail via online portals or remotely should have MFA as well. If a hacker attempts to log into an account that is protect by MFA, you will notice the attempt via the request for the second factor and be able to quickly take steps to protect your systems.

2. **Supported Systems.** Review your systems and identify any that are not fully patched or may be currently end-of-life. End-of-life equipment is that which is no longer supported by the manufacturer. In other words, the manufacturer does not provide any updates or security patches for the equipment and vulnerabilities are often exploited by attackers. In addition, if an attack occurs, data may be corrupted and unrecoverable, complicating efforts to restore systems. Also, ensure you have a process for identifying and applying critical security patches. Vulnerabilities are often made public through the Critical Vulnerability and Exposures (CVE[4]) program. This list is monitored by attackers, who then conduct automated scans to identify companies that have not patched the vulnerabilities. The attackers will then exploit the vulnerability to gain access to the system and perpetrate a cyberattack.
3. **Vendor Due Diligence.** Because small firms have limited resources, many outsource various cybersecurity requirements to vendors. Vendors include not just those who may provide services to help you protect your systems but also cloud and other hosted platforms. But vendors are at just as much risk of a cyberattack as are small law firms, and it is important that you conduct a thorough review of their security controls. Do they have a written information security program, and require their vendors to comply with the program? Do they have a security certification, such as ISO 27001[5] or a SOC2 certification?[6] Do they conduct regular internal and external vulnerability scans and penetration testing and address any issues? Are their systems up-

4. *See* CVE, cve.mitre.org/index.html; the CVE Program is intended to "identify, define, and catalog publicly disclosed cybersecurity vulnerabilities." CVE is sponsored by the U.S. Department of Homeland Security Cybersecurity and Infrastructure Agency.

5. *ISO/IEC 27001 Information Security Management*, ISO, https://www.iso.org/isoiec-27001-information-security.html (last visited Nov. 19, 2021).

6. *SOC 2®—SOC for Service Organizations: Trust Services Criteria*, AICPA, https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html (last visited Nov. 19, 2021).

ɔortals or remotely should have MFA as well. If
log into an account that is protect by MFA, you
pt via the request for the second factor and be
teps to protect your systems.
eview your systems and identify any that are not
ɔe currently end-of-life. End-of-life equipment is
· supported by the manufactuɪer. In other words,
not provide any updates or security patches for
nerabilities are often exploited by attackers. In
occurs, data may be corrupted and unrecover-
ɪrts to restore systems. Also, ensure you have a
and applying critical security patches. Vulner-
e public through the Critical Vulnerability and
ɜram. This list is monitored by attackers, who
ed scans to identify companies that have not
ties. The attackers will then exploit the vulner-
› the system and perpetrate a cybeɪattack.
Because small firms have limited resources,
s cybersecurity requirements to vendors. Ven-
hose who may provide services to help you
ɪt also cloud and other hosted platforms. But
ɪch risk of a cyberattack as are small law firms,
you conduct a thorough review of their secu-
ave a written information security program,
's to comply with the program? Do they have
uch as ISO 27001[5] or a SOC2 certification?[6]
ɪr internal and external vulnerability scans
ɪnd address any ɪssues? Are their systems up-

ɪtml; the CVE Program is intended to "ɪdentify, define,
ecurity vulnerabilities." CVE ɪs sponsored by the U.S.
'bersecurity and Infrastructure Agency.
'ecurity Management, ISO, https'//www.iso org/isoiec
t vɪsited Nov. 19, 2021).
rganizations: Trust Servɪces Criteɪɪa, AICPA, https://
ɪnceadvisoryservices/aɪcpasoc2report.html (last vɪsited

to-date and regularly patched? Do they conduct routine training for employees? Do they have backups in place that are segmented from their network, and have they tested the restoration process? Do they have cyber insurance in the event they experience an attack? There are other questions you may want to consider, but these are some of the most important to ask your vendors.[7]

4. **Vendor Contracts.** Once you have ɪdentified a vendor that meets your qualifications, carefully review the contract to ensure it has the appropriate protections in place. Many vendor contracts contain clauses that limit recovery of any damages to fees paid over a certaɪn period of tɪme. If your vendor suffers an attack that causes its systems to be unavailable for a significant period of time, or suffers a breach of your data, or an attack that causes you to lose all data, consider whether the contractual recovery will be sufficient. The contract should also require the vendor to have cyber insurance, include security controls, and require the vendor to provide information to you and cooperate with you should they suffer a cyberattack.
5. **Training.** You can spend as much money as you would like on security tools and programs, but ɪf you don't include traiɪɪing, the best protections will be for naught.[8] Often, security controls are bypassed or defeated because of human error, or a lack of recognitɪon or understanding of the risk. For exámple, one company had implemented MFA on its e-mail environment to protect access through the online portal. For the second "factor," the employee would receive a phone call requesting access to the account. An attacker compromised an employee's credentials and tried to log into the account. As a result, the employee started receiving a number of phone calls requesting they authorize access. The employee got tired of receiving the phone calls, and instead of contacting IT, authorɪzed access bypassing MFA.[9]

7. The American Bar Association Cybersecurɪty Task Force recently published a book to support small businesses with thɪrd-party rɪsks. *See* VENDOR CONTRACTING PROJECT: CYBERSECURITY CHECKLIST (2d ed. 2021), https://www.americanbar.org/products/ecd/ebk/411859099/.
8. See Chapter 13 *ɪnfra* for a more complete discussɪon of educatɪon and traɪning.
9. *Cybersecuɪɪɪty*, CISA, https'//www.cisa.gov/cybersecurity-training-exercises (last vɪsited Nov. 19, 2021)

Training is key and needs to be up-to-date and relevant. Regularly training employees on recognizing and responding to suspicious cyber activity will help you protect your network. Your employees are the first ones who may see that an attack is occurring and let you know so you can take steps to mitigate damage and protect your systems and your clients.

Training should touch on topics like social engineering, vishing,[10] smishing,[11] and phishing.[12] Employees should also be instructed not to open attachments in e-mails from unfamiliar senders. Even if an e-mail is from a familiar name, but it seems peculiar or unexpected, don't open any attachment or click on a link in the e-mail; contact the sender and ask if they sent the e-mail. The attachment or the link may release malware onto the computer. If anyone receives a pop-up that their computer is "infected with a virus," they should know that this is an actual attempt to infect their computer, and it should be ignored or deleted.

6. **Written Information Security Program.** Establish a written information security program (often called a WISP) that outlines the security controls for your systems. The WISP should contain policies that direct employees what they can and cannot do with their firm computer, or while they are in the office (or, if you are a solo practitioner, what you should or shouldn't do). The WISP should also outline the security controls for your security systems and those that vendors are required to follow. Clients often require firms to provide information about

10. Vishing is a combination of voice and phishing, and is the attempt to obtain personal information through telephone systems. *See* Genevieve Bookwalter, *What Is Vishing? Tips for Spotting and Avoiding Voice Scams*, NORTON, https://us.norton.com/internetsecurity-online-scams-vishing.html (last visited Nov 19, 2021).

11 Smishing is the attempt by an attacker to obtain personal information via text messages. *See Avoid the Temptation of Smishing Scams*, FED. COMMC'NS COMM'N (Nov. 9, 2018), https://www.fcc.gov/avoid-temptation-smishing-scams.

12. Phishing is an attempt by an attacker to obtain your personal information via email or text messages to gain access to your accounts. *See How to Recognize and Avoid Phishing Scams*, FED. TRADE COMM'N: CONSUMER INFO. (May 2019), https://www consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.

their security programs, and may request that you provide proof that you have written policies and procedures.

There are a variety of security controls the WISP should address. For instance, you should include a password management policy that requires complex passwords,[13] which are changed on a rolling basis. Part of your password management policy should include immediate cancellation of a password of any employee (including attorneys) who leaves the firm. If any vendors have a password that allows access to your systems, these should be rotated on a routine basis and be terminated if the relationship ends. Set passwords to "lock out" after a set number of failed attempts. And as noted earlier, MFA should be enabled on any remote access.

7. **Backups.** Backups are critical for the resiliency of your system. Establish backups so that you can recover quickly in the event of a physical or security disaster. Attackers frequently gain access to a system and, if they can access it, delete backups. Review your backup configuration to make sure the backups are segmented from your network. If you rely on cloud services or other vendors, make sure they also have a robust backup protocol. Ensure access to the cloud backup is protected by MFA. Attackers will gain access to your system and monitor your activity. One company discovered that during this process, the attackers learned how the backups were set up, obtained the password to its cloud backup, deleted the backups, and then encrypted its systems. Also, make sure that you and your colleagues actually store data on the cloud provider's site, and don't just save items to the local drive. A device may fail due to a mechanical problem, such as a crashed hard drive. Or, a criminal may penetrate your workstation, take your data hostage, and demand a large ransom. Occasionally test the restoration process as well; make sure it works and the restoration process takes hours, not days.

13. *See* Whitney Merrill, *Advanced Password Tips and Tricks*, FED. TRADE COMM'N: CONSUMER INFO. (July 30, 2015), https://www.consumer.ftc.gov/blog/2015/07/advanced-password-tips-and-tricks.

8. **Security Incident or Data Breach Preparation.** As mentioned at the beginning of this chapter, it isn't "if" you will experience a cyberattack, but rather "when." Preparation is key, and helps mitigate damages and protect your brand. You should have an incident response plan (IRP) that outlines the steps to take in the event you experience a cyberattack. The IRP should also include key points of contact, such as your cyber insurer. Print the plan out and practice it—if your systems are encrypted, you won't be able to access the plan and having a printed copy is key.[14]
9. **Cyber Insurance.** You've done all of this to enhance your cybersecurity, but you still should have insurance to cover you in the event of a disaster. The terms of cyber insurance policies tend to vary from company to company, and, like any other contract you review, you should make sure that you have a clear understanding of all the provisions.[15] For example, precisely when will coverage start? In some cases, insurance companies may take the position that a loss was due to a breach that occurred prior to the effective date of the policy. Make sure that there is agreement on what constitutes "unauthorized access" to your system. Does it include lost laptops? Does it include someone being tricked into providing a password? Make sure that there is agreement on the level of security that the insurance company considers the minimum acceptable level. Will the policy provide the type of services needed to help you recover from a security incident? Will it help you restore data and establish new (and presumable more robust) security protocols? Will the amount of coverage be sufficient for remediation, or for paying a ransom demand?
10. **Cybersecurity and Data Compliance.** Every year, more laws are enacted or amended that include cybersecurity or privacy requirements for organizations that either do business in that state or in a particular industry. Your clients may have to comply with these requirements if they operate in certain states or industries, and through contract you may be required to do so as well. Although the default requirement

14. See Chapter 15 of this Handbook for further discussion of incident preparation.
15. See Chapter 16 of this Handbook for further discussion of cyber insurance

y Incident or Data Breach Preparation. As mentioned at the ng of this chapter, it isn't "if" you will experience a cyberattack, ıer "when." Preparation is key, and helps mitigate damages and your brand. You should have an incident response plan (IRP) tlines the steps to take in the event you experience a cyberat- ıe IRP should also include key points of contact, such as your ısurer. Print the plan out and practice it—if your systems are ed, you won't be able to access the plan and having a printed key.[14]

ısurance. You've done all of this to enhance your cybersecu- t you still should have insurance to cover you in the event of ter. The terms of cyber insurance policies tend to vary from ny to company, and, like any other contract you review, you make sure that you have a clear understanding of all the pro- .[15] For example, precisely when will coverage start? In some nsurance companies may take the position that a loss was due each that occurred prior to the effective date of the policy. ure that there is agreement on what constitutes "unauthorized to your system. Does it include lost laptops? Does it include ıe being tricked into providing a password? Make sure that agreement on the level of security that the insurance company rs the minimum acceptable level. Will the policy provide the services needed to help you recover from a security incident? ıelp you restore data and establish new (and presumable more security protocols? Will the amount of coverage be sufficient ediation, or for paying a ransom demand?

curity and Data Compliance. Every year, more laws are enacted ıded that include cybersecurity or privacy requirements for ıtions that either do business in that state or in a particular . Your clients may have to comply with these requirements if rate in certain states or industries, and through contract you equired to do so as well. Although the default requirement

er 15 of this Handbook for further discussion of incident preparation
er 16 of this Handbook for further discussion of cyber insurance

is that all client communications or attorney work product should be maintained in confidence,[16] other data that may require additional protections or controls (e.g., Intellectual Property, International Traffic in Arms Regulations, information related to acquisitions, or personally identifiable information) should be identified and appropriately protected (e.g., as per Health Information Portability and Accountability Act, Payment Card Industry Data Security Standards, Gramm-Leach-Bliley Act, Family Educational Rights and Privacy Act, or state law).

11. **Other Security Controls.** There are a number of other security controls you should consider implementing. For instance, encryption technology is much less expensive today than it was years ago, and in many instances is included on new devices at no additional cost. Make sure your laptops or workstations are encrypted and ensure any smartphones or other mobile devices connecting to your network are encrypted. Determine whether it is feasible for databases containing sensitive information to be encrypted as well. If you frequently handle highly sensitive information, set up secure file transfer methods for sharing documents with clients or others who may need access. An up-to-date antivirus or endpoint threat detection program should be installed on all devices, including servers, that can be connected to the firm network. You should have a spam filter enabled for e-mails, and employees should be instructed not to install programs on firm computers without approval. Talk to your IT provider about remote methods of connecting to your systems. The most common way systems are compromised is through insecure remote connection protocols.
12. **Document Retention Policy.** If you don't need it, don't keep it. Most document retention policies refer only to how long you may be required to keep information, they generally don't include a requirement to delete data. But the less data you have on your systems, the

16 MODEL RULES OF PRO. CONDUCT r 1.6, Confidentiality of Information. "(a) 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)."

less information you have to protect. Remove data (and paper files) that no longer need to be saved (with consent of clients if it is client information). The less information you have, the smaller the footprint that you need to protect.

Small firms must recognize that they are just as much of a target as larger firms for a cyberattack, and the impact could be even more devastating because small firms lack the IT resources and overall funding of larger firms. Although the preceding list might feel overwhelming, many of the suggestions can be implemented at little to no cost. And overall, the cost of a cyberattack is much more expensive than taking the steps now to protect your systems, your data, and your clients.