January 28, 2019
TECHREPORT 2018

2018 Cybersecurity

David G. Ries

Security breaches are so prevalent that there is a new mantra in cybersecurity today—it's "when, not if" a law firm or other entity will suffer a breach. In an address at a major information security conference in 2012, then-FBI director Robert Mueller put it this way:

> "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."

Mueller's observation continues to be true today for attorneys and law firms as well as for small businesses through large global companies. There have been numerous reports for over a decade of law firm data breaches in the popular and legal press—print and online. The FBI has reported that law firms are often viewed as "one-stop shops" for attackers (with information on multiple clients) and it has seen hundreds of law firms being increasingly targeted by hackers. Law firm breaches have ranged from simple (like those resulting from a lost or stolen laptop or mobile device) to highly sophisticated (like the deep penetration of a law firm network, with access to everything, for a year or more).

New York Ethics Opinion 1019 warned attorneys in May 2014 about this threat environment:

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

Several years later, ABA Formal Opinion 477, "Securing Communication of Protected Client Information" (May 11, 2017), observed:

> "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."

Most recently, ABA Formal Opinion 483, "Lawyers' Obligations After an Electronic Data Breach or Cyberattack" (October 17, 2018) starts with the following observations about current threats:

> "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 regular regularly divide business entities into two categories: those that have been hacked and those that will be."

The ABA's *2018 Legal Technology Survey Report* explores security threats and incidents and safeguards that reporting attorneys and their law firms are using to protect against them. As in past years, it shows that many attorneys and law firms are employing some of

the safeguards covered in the questions and generally increasing use of the safeguards over time. However, it also shows that many are not using security measures that are viewed as basic by security professionals and are used more frequently in other businesses and professions.

Some attorneys and law firms may not be devoting more attention and resources to security because they mistakenly believe "it won't happen to me." The increasing threats to attorneys and law firms and the reports of security breaches should dispel this mistaken viewpoint. Significantly, 23% of respondents overall reported this year that their firm had experienced a data breach at some time.

Data security is addressed most directly in *2018 Survey,* "Volume I: Technology Basics & Security." It is further addressed in "Volume IV: Marketing and Communications Technology," and "Volume VI: Mobile Lawyers." This *TECHREPORT* reviews responses to the security questions in this year's Survey and discusses them in light of both attorneys' duty to safeguard information and standard information security practices. Each volume includes a Trend Report, which breaks down the information by size of firm and compares it to prior years, followed by sections with more detailed information on survey responses. This gives attorneys and law firms (and clients) information to compare their security posture to law firms of similar size.

Attorneys' Duty to Safeguard Information

The ethics rules require attorneys to take competent and reasonable measures to safeguard information relating to clients (ABA Model Rules 1.1 and 1.6 and Comments). These duties are covered in these rules and comments and in the recent ethics opinions like the ones discussed above. Attorneys also have common law duties to protect client information and often have contractual and regulatory obligations to protect information relating to clients and other personally identifiable information, like health and financial information. These duties present a challenge to attorneys using technology because most are not technologists and often lack training and experience in security. Compliance requires attorneys to understand limitations in their knowledge and obtain sufficient information to protect client information, to get qualified assistance if necessary, or both. These obligations are minimum standards —failure to comply with them may constitute unethical or unlawful conduct. Attorneys should aim for security that goes beyond these minimums as a matter of sound professional practice and client service.

Recognizing the Risk

Information security starts with an inventory and risk assessment to determine what needs to be protected and the threats that it faces. The inventory should include both technology and data. You can't protect it if you don't know that you have it and where it is.

Comment [18] to Model Rule 1.6 includes a risk-based approach to determine reasonable measures that attorneys should employ. The first two factors in the analysis are "the sensitivity of the information" and "the likelihood of disclosure if additional safeguards are not employed." This analysis should include a review of security incidents that an attorney or law firm has experienced and those experienced by others—generally and in the legal profession. The *2018 Survey* includes information about threats in its questions about security breaches.

The next factors in the risk analysis cover available safeguards. Comment [18] to Model Rule 1.6 includes them in the risk analysis for attorneys for determining what is reasonable:

> "...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)."

Comment [18] uses a risk-based approach that is now standard in information security. The *2018 Survey* includes information about the available safeguards that various attorneys and firms are using.

The *2018 Survey* reports that about 23% of respondents overall reported that their firms had experienced a security breach at some point. The question is not limited to the past year, it's "ever." A breach broadly includes incidents like a lost/stolen computer or smartphone, hacker, break-in, or website exploit. This compares with 22% last year, 14% in 2016, 15% in 2015, 14% in 2014, and 15% in 2013—an increase of 8% in 2017 after being basically steady from 2013 through 2016.

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

Larger firms have more people, more technology, and more data, so there is a greater exposure surface, but they also should have more resources to protect them. It is difficult to tell the completeness of larger firm's responses on breaches because the percentage of those reporting that they "don't know" about breaches (18% overall) directly goes up with firm size—reaching 57% in firms with 100-499 attorneys and 61% in firms with 500+. This makes sense because attorneys in medium and large firms may not learn about security incidents that don't impact the entire firm, particularly minor incidents and ones at remote offices.

The majority of respondents—60%—reported that their firm had not experienced a breach in the past. Hopefully, this does not include firms that have experienced a security breach and never detected it. Another common saying in security today is that there are two kinds of companies: Those that have been breached and know it, and those that have been breached but don't know it. The same is likely true for law firms.

The most serious consequence of a security breach for a law firm would most likely be unauthorized access to sensitive client data (although the loss of data would also be very serious). The *2018 Survey* shows a very low incidence of this result for firms that experienced a breach—about 6% overall, up from 1% last year. The reports of unauthorized access to sensitive client data by firms that experienced a breach is 11% for solos (up from none last year); 6-8% for firms with 2-9, 10-49, and 50-99; none reported for firms with 100+. While the percentages are low, any exposure of client data can be a major disaster for a law firm and its clients.

The information on breaches with exposure of client data is incomplete because almost 7% overall report that they don't know about the consequences, with "don't know" responses increasing from none for solos to 38% for firms of 500+. The uncertainty is increased by the high percentage of respondents (18%), discussed above, who don't even know whether their firm experienced a data breach.

Unauthorized access to non-client sensitive data is 6% overall, with 8% for solos, 5% for firms with 2-9, 10% for firms with 10-49, 8% for firms with 50-99, 5% for firms of 100-499, and none for firms with 500+.

The other reported consequences of data breaches are significant. Downtime/loss of billable hours was reported by 41% of respondents; consulting fees for repair were reported by 40%; destruction or loss of files by 11%, and replacement of hardware/software reported by 27% (percentages for firms that experienced breaches). Any of these could be very serious, particularly for solos and small firms that may have limited resources to recover. No significant business disruption or loss was reported by 65% overall.

About 9% overall responded that they notified a client or clients of the breach. The percentage reporting notice to clients ranges from 11% for solos, 8% for firms with 2-9, 7% for firms with 10-49, 17% for firms with 50-99, none for firms with 100-499 and 19% for firms with 500+. This is equal to or in excess of the reported incidence of unauthorized access to client data for firms of each size, consistent with the view that ethical and common law obligations require notice to clients.

Overall, 14% of respondents that experienced a breach reported that they gave notice to law enforcement, ranging from 13% for solos, 10% with 2-9 attorneys, 20% of firms with 10-49, 25% of firms with 50-99, 5% of firms with 100-499 attorneys to 25% of firms with 500+.

The *2018 Survey* also inquired whether respondents ever experienced an infection with viruses/spyware/malware. Overall, 40% reported infections, 37% reported none, and 23% reported that they don't know. Reported infections were greatest in firms with 10-49

attorneys (57%) and 2- 9 (48%), and lowest in firms with 500+ (20%). Infections can cause serious consequences, including compromise of confidentiality and loss of data. With over one third of respondents reporting infections (down from almost half last year), strong safeguards to protect against them, including up to date security software, using current versions of operating systems and software, promptly applying patches to the operating system and all application software, effective backup, and training of attorneys and staff are clearly warranted.

Security Programs and Policies

At the ABA Annual Meeting in August, 2014, the ABA adopted a resolution on cybersecurity that "encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations and is tailored to the nature and scope of the organization and the data and systems to be protected." The organizations covered by it include law firms.

A security program should address people, policies and procedures, and technology. All three areas are necessary for an effective program. Security should not be left solely to IT staff and tech consultants. In addition to measures to prevent security incidents and breaches, there has been a growing recognition that security includes the full spectrum of measures to identify and protect information assets and to detect, respond to, and recover from data breaches and security incidents. Security programs should cover all of these functions.

An important initial step in establishing an information security program is defining responsibility for security. The program should designate an individual or individuals responsible for coordinating security—someone must be in charge. It should also define everyone's responsibility for security, from the managing partner or CEO to support staff.

While a dedicated, full-time Chief Information Security Officer is generally only appropriate (and affordable) for larger law firms, every firm should have someone who is responsible for coordinating security. The larger the firm, the more necessary it is to have a full-time security officer or someone who is to dedicate an appropriate part of their time and effort to security. The *2018 Survey* asks who has primary responsibility for security in respondents' firms. As expected, responses vary by size of firm. The respondent has primary responsibility in solo firms (84%), the respondent or an external consultant/expert in firms of 2-9 attorneys (27% and 33%, respectively); IT staff for firms of 10-49 attorneys (41%) and 50-99 (47%), a chief information officer in firms of 100-499 (56%) and firms of 500+ (62%). A small percentage (2%) report that nobody has primary responsibility for security—a high-risk situation.

The *2018 Survey* asks respondents about a variety of technology-related policies, rather than about an overall comprehensive information security program. Attorneys and law firms should view these kinds of policies as part of a coordinated program rather than individually.

According to the *2018 Survey*, 53% of respondents report that their firms have a policy to manage the retention of information/data held by the firm, 50% report a policy on email use, 44% for internet use, 41% for computer acceptable use, 37% remote access, 38% for social media, 21% personal technology use/BYOD, and 32% for employee privacy. The numbers generally increase with firm size. For example, about 33% of solo respondents report having an information/data retention policy, increasing to 51% in firms with 2-9, 60% with 10-49, 77% with 50-99, and approximately 90% in 100+ attorneys.

Two responses that raise a major security concern are those that report having no policies (29% overall) and those reporting that they don't know about security policies (7%). There is a clear trend by firm size in the responses of having no policies. There are no respondents in firms of 100+ attorneys reporting none. The percentage with none generally decreases by firm size, ranging from 3% of firms with 50-99, 6% with 10-49, 25% in firms with 2-9, to 58% of responding solos. While it is understandable that solos and smaller firms may not appreciate the need for policies, all firms should have policies, appropriately scaled to the size of the firm and the sensitivity of the data.

Incident response is a critical element of an information security program. Overall, 25% report having an incident response plan. The percentage of respondents reporting that they have incident response plans varies with firm size, ranging from 9% for solos and 16% for firms with 2-9 to approximately 70% forms with 100+. As with a comprehensive security program, all attorneys and law firms should have an incident response plan scaled to the size of the firm. For solos and small firms, it may just be a checklist plus who to call for what, but they should have a basic plan.

Security awareness is a key to effective security. There cannot be effective security if users are not trained and do not understand the threats, how to protect against them, and the applicable security policies. Obviously, they can't understand policies if they don't even know whether their law firm has any policies.

In accordance with the ABA resolution on cybersecurity programs (and generally accepted security practices), all attorneys and law firms should have security programs tailored to the size of the firm and the data and systems to be protected. They should include training and constant security awareness.

Security Assessments and Client Requirements

Clients are increasingly focusing on the information security of law firms representing them and using approaches like required third-party security assessments, security requirements, and questionnaires.

The increased use of security assessments conducted by independent third parties has been a growing security practice for businesses and enterprises generally. Law firms have been slow to adopt this security tool, with only 28% of law firms overall reporting that they had a full assessment, but it increased from 27% last year and 18% in 2017. Affirmative responses generally increase by size of firm.

Third-party assessments are often conducted for law firms only when a client requests it or requires it. Overall, 11% report that a client or prospective client has requested an audit or other review. The percentage of firms reporting a client request gradually goes up by size of firm, from 2% for solos to 39% for firms of 500+.

Overall, 34% of respondents report that they have received a client security requirements document or guidelines. Firms receiving them generally increase by size of firm, from 15% of solos to about 66% with 100+ attorneys. There is a growing recognition in the information security profession of the importance of securing data that business partners and service providers can access, process, and store. This includes law firms. In March of 2017, the Association of Corporate Counsel (ACC) published the *Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information* that provides a list of baseline security measures and controls that legal departments can consider in developing requirements for outside counsel. Attorneys and law firms are likely to continue to face increasing client requirements for security.

Cyber Insurance

As the headlines continue to be filled with reports of data breaches, including law firms, there has been a growing recognition of the need for cyber insurance. Many general liability and malpractice policies do not cover security incidents or data breaches. The percentage of attorneys reporting that they have cyber liability coverage is small but has been increasing—34% overall (up from 27% in 2017, 17% in 2016, and 11% in 2015). It gradually increases from 27% for solos to about 35-45% for midsize firms, then drops to 23% for firms of 500+. In addition to cyber liability insurance, covering liability to third parties, there is also coverage available for first-party losses to the law firm (like lost productivity, data restoration, and technical and legal expenses). A review of the need for cyber insurance coverage should be a part of the risk assessment process for law firms of all sizes.

Security Standards and Frameworks

A growing number of law firms are using information security standards and frameworks, like those published by the International Organization for Standardization (ISO), the National Institute of Standards and Technology (NIST), and the Center for Internet Security (CIS). They provide consensus approaches to a comprehensive information security program. Some firms use them as guidelines for their security programs, while a smaller group of firms seek formal security certification. The *2018 Survey* asks whether respondents' firms have received a security certification. Overall, only 9% report that they have received certification, with a low of 3% for solos and a high of 27% for firms with 500+.

Authentication and Access Control

Authentication and access controls are the first lines of defense. They are the "keys to the kingdom"—controlling access to networks, computers, and mobile devices.

The *2018 Survey* includes a general question about mandatory passwords without specifying the access for which they are required. Overall, 68% of respondents report using mandatory passwords. They are required by 53% of solos, 71% of firms of 2-10 attorneys, and about 80% or higher for larger firms. This question does not ask about other forms of authentication like fingerprints or facial recognition. Some form of strong authentication should be required for access to computers and networks for all attorneys and all law firms.

For laptops, a strong majority of responding attorneys—nearly all—report that they use access controls. Overall, 98% report using passwords, with 99% for solos, 98% for firms of 2-9 attorneys, 94% for firms of 10-49, and firms of 50-500+ at 100%. In addition, 19% overall report using other authentication, which would include fingerprint readers, facial recognition, and other alternatives. While this might suggest that all attorneys use some form of access control (98% + 19%), that is not the case. About 1% report that they use none of the listed laptop security measures. The response of "none" only includes solos and firms 10-49 attorneys. As noted above, larger firms report 100% use of passwords for laptops.

Use of authentication controls on smartphones is similar to those on laptops. Reported use of passwords is 92% overall—generally increasing with firm size from 87% for solos to 100% for firms of 500+. Firms of other sizes range from about 90% to 99%. Use of other authentication is 40% overall, while 5% reporting none of the listed security measures.

For both laptops and smartphones (as well as other mobile and portable devices), all attorneys should be using strong passwords or other strong authentication.

Most, if not all, attorneys need multiple passwords for a number of devices, networks, services, and websites—for both work and personal use. It is recommended that users have a different, strong password for each device, network, service, and website. While password standards are evolving—stressing length over complexity—it is very difficult, or impossible, to remember numerous passwords. Password management tools allow a user to remember a single, strong password for the tool or locker with automatic access to the others. Respondents report that 24% overall use password management tools. 16% report that they don't know. It is unlikely that respondents who don't know are using these tools because a user would have to know that they are using a single password to access others. There is some difference in use by size of firm, ranging from a low of 16% for firms with 50-99 attorneys to a high of 30% for firms with 100-499.

Encryption

Encryption is a strong security measure that protects data in storage (on computers, laptops, smartphones, tablets, and portable devices) and transmitted data (over wired and wireless networks, including email). Security professionals view encryption as a basic safeguard that should be widely deployed. It is increasingly being required by law for personal information, like health and financial information. The recent battle between the FBI and Apple and the current debate about mandated "backdoors" to encryption for law enforcement and national security show how strong encryption can be for protecting sensitive data. The *2018 Survey* shows that use by attorneys of the covered encryption tools has been growing, but its use is limited.

Full-drive encryption provides strong protection for all of the data on a server, desktop, laptop, or portable device. The data is readable only when it is decrypted through use of the correct password or other access control. Respondents report an overall use of full-drive encryption of only 24% (up from 21% last year and 15% in 2016), ranging from 15% for solos to about 48% for firms of 100+, with percentages increasing by firm size. File encryption protects individual files rather than all the data on a drive or device. Reported use of file encryption is higher than full disk at 46% overall, ranging from 36% for solos to 72% in firms of 500+. This question is general and is not broken down in Volume I of the *2018 Survey* by servers, desktops, laptops, smartphones, etc. As discussed below, all attorneys should use encryption on laptops, smartphones, and mobile devices. While some law firms are starting to encrypt desktops and firm servers, it is not yet a common practice.

Volume VI of the *2018 Survey* has separate questions for laptops and smartphones. For laptops, 25% overall report using file/data encryption and 18% report using hard drive encryption. Both of these numbers are down slightly from last year. File/data protection relies on the user to encrypt individual files or to put sensitive information in an encrypted file or partition on the drive. Full-drive encryption provides broader protection because it protects all data on the drive. Use of full-drive encryption for laptops does not vary directly with firm size—reported use is 18% for solos, 13% for firms with 2-9, 26% for firms with 10-49, 18% of firms with 50-99, 30% of firms with 100-499, and only 15% of firms with 500+ attorneys.

The *2018 Survey* also reported on additional security measures for laptops, like remote data wiping (12% overall) and tracking software (7% overall). These kinds of measures can provide additional security, but should not be a substitute for strong authentication and encryption.

Use of encryption on smartphones appears to be significantly under-reported by attorneys responding to the *2018 Survey*, as in past years. Respondents report an overall use of encryption of smartphones by only 18%. However, 72% overall of attorneys who use smartphones for work report using iPhones and 94% report that they use password protection on their smartphones. On current iPhones, encryption is automatically enabled when a PIN or passcode is set. Google is also moving to automatic encryption with a PIN or swipe pattern for Android devices. It appears that many attorneys are using encryption on their smartphones without knowing it. Encryption can be that easy! Encryption of laptops may also be under-reported because it can be transparent to the user if it has been enabled or installed by a law firm's IT staff or a technology consultant.

Verizon's *2014 Data Breach Investigation Report* concludes that "encryption is as close to a no-brainer solution as it gets" for lost or stolen devices. Attorneys who do not use encryption on laptops, smartphones, and portable devices should consider the question: Is failure to employ what many consider to be a no-brainer solution taking competent and reasonable measures?

Secure email is another safeguard with limited reported use by responding attorneys. Overall, 29% of respondents reported that they use encryption of email for confidential/privileged communications/documents sent to clients (down from 36% last year). This ranges from 19% for solos, gradually increasing to 70% with firms of 50-99 and 73% for firms of 500+. Firms of 100-499 are an exception, with only 47% reporting use of encryption for email. Another question asks about registered/secure email, which appears to also include encryption. Overall, 18% report using registered/secure email, increasing directly with firm size from 12% for solos to 36% for firms with 500+. If there is no overlap between this response and the use of encryption, the overall percentage using email security would be 47% overall, increasing with firm size to 100% of firms with 500+.

Email encryption has now become easy to use and inexpensive with commercial email services. Google and Yahoo, at least in part driven by the disclosures about NSA interception, announced in 2014 that they would be making encryption available for their email services. In its announcement, Google compared unencrypted email to a postcard and encryption as adding an envelope. This postcard analogy has been used by security professionals for years. Hopefully, the percentages of attorneys reporting that they have added the envelopes, where appropriate, will grow in future survey results.

During the last several years, some state ethics opinions have increasingly expressed the view that encryption of email may sometimes be required to comply with attorneys' duty of confidentiality. On May 11, 2017, the ABA issued Formal Opinion 477, Securing Communication of Protected Client Information. The Opinion revisits attorneys' duty to use encryption and other

safeguards to protect email and electronic communications in light of evolving threats, developing technology, and available safeguards. It suggests a fact-based analysis and concludes "the use of un-encrypted routine email generally remains an acceptable method of lawyer-client communication," but "particularly strong protective measures, like encryption, are warranted in some circumstances." It notes that attorneys are required to use special security precautions, like encryption, "when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security."

If encrypted email is not available, a strong level of protection can be provided by putting the sensitive information in an encrypted attachment instead of in the text of the email. In current versions of Microsoft Office, Adobe Acrobat, and WinZip, setting a password for the document encrypts it. While password protection of documents is not as strong as encryption of a complete email and attachments because it depends on the strength of the password, it is much more secure than no encryption. If this approach is used, it is important to securely provide the passwords or passphrase to the recipient(s), preferably through a different communication channel like a phone call or text message (and certainly not in the email used to send the document).

Overall, a low percentage of respondents report using password protection for documents. There is not a pattern by firm size, with a low of 12% reported by solos and a high of 35% reported by firms of 100-499.

It has now reached the point where all attorneys should generally understand encryption and have encryption available for use in appropriate circumstances.

Some Basic Security Tools

In addition to authentication and encryption, the *2018 Survey* asks about various security tools that are available to responding attorneys. Most, if not all, of these tools are security basics that should be used by all attorneys and law firms.

The most common tool is the spam filter, used by 87% of respondents. This may be under-reported because most email service providers have at least basic spam filters. Spam filters can be a strong first line of defense against phishing (malicious emails that try to steal information or plant malware). Filters are only part of the defense that weeds out some phishing emails but are an important first step.

Other tools with high reported use include anti-spyware (80%), software-based firewalls (80%), antivirus for desktops/laptops (73%), for email (69%), for networks (66%), and hardware firewalls (57%). Use of intrusion detection and prevention systems is reported by about 33% of respondents overall. There has been a growing trend for a number of years to use security suites that combine some of these tools like malware protection, spyware protection, software firewalls, and basic intrusion protection in a single tool. Availability of the various security tools is generally stable across firms of all sizes, with increases for some of them with the size of the firm. For all of these security tools, the use by firms should be 100%. There is a generally low incidence of "don't know" responses for these tools, about 7% overall.

Remote Access

Approximately 90% of respondents reported that they remotely access work assets other than email, like applications and files, consistent with today's mobile practice of law. 39% report regular use of remote access, 31% report occasional use, and 19% report "seldom." Reported use generally increases with firm size, reaching 68% for firms of 500+. Respondents report using the following security measures: web-based applications (42%), virtual private networks (VPNs) (37%), remote access software (30%), and other (10%). Security for remote access is critical because it can provide unauthorized access for outsiders (to the communication or network) if it is not properly secured with an encrypted communication connection and strong authentication. There is a growing practice of using multifactor authentication or two-step verification for authentication in remote access. It requires a second method of authentication, in addition to a password, like a set of numbers transmitted to a smartphone or generated by an app. Multiple inexpensive and easy-to-use options are available.

Wireless Networks

Public wireless (WiFi) networks present a high-security risk, particularly if they are open, as in not requiring a password for connection. Without appropriate security measures, others connected to the network—both authorized users and attackers—may be able to intercept or view data and electronic communications transmitted over the network. The *2018 Survey* asks about security measures that attorneys use when accessing public wireless networks. 31% report that they do not use public wireless networks. Overall, 38% report that they use a VPN (a technology that provides an encrypted connection over the internet or other networks), 20% report that they use remote access software, 15% report that they use website-provided SSL/HTTPS encryption, and 0.6% report using other security measures. The remaining 15% are living dangerously, reporting that they use none of the security measures.

Cell carriers' data networks generally provide stronger security than public WiFi, either with access built into a smartphone, tablet, or laptop, or by using a smartphone, tablet, or separate device as a personal hotspot.

Up-to-date equipment and secure configuration (using encryption) are also important for a law firm and home wireless networks.

Disaster Recovery/Business Continuity

Threats to the availability of data can range from failure of a single piece of equipment to a major disaster like a fire or hurricane. An increasing threat to attorneys and law firms of all sizes is ransomware, generally spread through phishing. It encrypts a user's or network's data and demands ransom (to be paid by Bitcoin) for release of the decryption key. Effective backup, which is isolated from production networks, can provide timely recovery from ransomware.

Overall, 17% of respondents report that their firm had experienced a natural or man-made disaster, like a fire or flood. The highest incidence, about 32%, was in firms of 50-99 and 500+. The lowest reported incidence was for solos at 10%, with the rest were between these numbers. Disasters of this kind can put a firm out of business temporarily or permanently. These positive responses, from 10% to 32% of respondents, and the potentially devastating results demonstrate the importance for law firms of all sizes to be prepared to respond and recover.

Despite this clear need, only 40% overall of responding attorneys report that their firms have a disaster recovery/business continuity plan. Firms with a plan generally increase with the size of the firm, ranging from 22% of solos to over 85% of firms with 50-99 and 500+ attorneys. As with comprehensive security programs, all law firms should have a disaster recovery/business continuity plan, appropriately scaled to its size.

In the equipment failure area, 34% of respondents reported that their firm experienced a hard drive failure, while 44% reported that they did not. The remainder reported that they do not know, with the "don't knows" increasing by firm size. In firms of 500+, 73% responded that they don't know. In firms of 100-499, it was 61%. It is very likely that most large firms have suffered multiple hard drive failures, just not known by the individual responding attorneys. Even limiting the analysis to known hard drive failures, they have impacted about one-third of respondents. That's a high risk, particularly considering the potential consequences of lost data, and all attorneys and law firms should implement backup and recovery measures.

Backup of data is critical for business continuity, particularly with the current epidemic of ransomware. Fortunately, most firms report that they employ some form of backup. Only 1.5% report that they don't back up their computer files. 21% of respondents report that they don't know about backup. The most frequently reported form of backup is external hard drives (38%), followed by offsite backup (30%), online backup (30%), network attached storage (15%), USB (9%), tape (7%), RAID (7%), CDs (4%), and DVDs (4%).

The *2018 Survey* responses show that 49% of respondents back up once a day, 22% more than once a day, 11% weekly, 5% monthly, and 2% quarterly. 8% report that they don't know, with unknowns increasing with firm size. Attorneys and firms that don't back up on a daily basis, or more frequently, should reevaluate the risk in light of ransomware, hardware failures, disasters, and other incidents reported in the *2018 Survey*.

Conclusion

The *2018 Survey* provides a good overview, with supporting details, of what attorneys and law firms are doing to protect confidential information. Like the last several years, the data generally shows increasing attention to security and increasing use of the covered safeguards but also demonstrates that there is still a lot of room for improvement. Attorneys and law firms who are behind the reporting attorneys and firms on safeguards should evaluate their security posture to determine whether they need to do more to provide, at minimum, competent and reasonable safeguards—and hopefully more. Those who are in the majority on safeguards, or ahead of the curve, still need to review and update their security as new technology, threats, and available safeguards evolve over time. Effective security is an ongoing process, not just a "set it and forget it" effort. All attorneys and law firms should have appropriate comprehensive, risk-based security programs that include appropriate safeguards, training, periodic review and updating, and constant security awareness.

Authors

ENTITY:

LAW PRACTICE DIVISION, LEGAL TECHNOLOGY RESOURCE CENTER

TOPIC:

CYBERSECURITY, TECHNOLOGY