November 29, 2022 **TECHREPORT 2022**

# 2022 Cybersecurity

John W. Simek

Share:

Cybersecurity is a nemesis for law firms these days. We can't seem to go a single day without hearing about some sort of security event such as a ransomware attack, data breach, newly discovered vulnerability, or some misuse of our information. It will make your head hurt trying to keep up with everything. One helpful tool is to understand the current threats and trends in the cyber world. There are many industry reports, surveys and statistics to give us guidance.

One resource specific to the legal profession is the ABA's *2022 Legal Technology Survey Report*. The survey results are provided in five volumes.

- Online Research
- Technology Basics & Security
- Law Office Technology
- Marketing & Communication Technology
- Litigation Technology & E-Discovery

Cybersecurity items are covered in the "Technology Basics & Security" volume of the survey. This Cybersecurity *TechReport* is a partial summarization of the detailed responses contained in the 60 plus page volume.

## Technology Competency

Attorneys have many ethical duties as it relates to the practice of law, especially as it relates to technology. Being technically competent is certainly an important requirement, but how is that achieved? As part of a lawyer's basic technology competency requirement, 68% of respondents reported having to stay abreast of the benefits and risks of technology. Interestingly, solo attorneys are most likely (77%) than the other groups to stay abreast of the benefits and risks of technology. This means training is an important part of the success of your law practice.

According to the *2022 Survey*, 75% of all respondents reported having some type of training available at their firm. Technology training increased along with firm size with 32% of solos having training available at their firm, followed by 64% for firms of 2-9 attorneys, 79% for firms of 10-49 attorneys, 93% for firms of 50-99 attorneys and 100% for firms of over 100 attorneys.

The training shouldn't focus only on technology used by the firm. These days, cybersecurity awareness training should be on every firm's calendar at least once a year and more if possible. The firm's

cyberinsurance carrier will likely require cybersecurity awareness training for employees. If not a specific insurance requirement, the carriers are certainly asking about it on the initial cyber policy application and renewal questionnaires.

According to the 2021 Verizon Data Breach Investigation Report, phishing was present in 36% of breaches. Other reports show that over 90% of cyber attacks begin with a phishing email and more than 97% of users cannot recognize a sophisticated phishing email. These stats alone make it clear why your firm must have cybersecurity training.

## Technology Policies

It is imperative that your firm have documented policies. Each firm is different, but some of the policies may include such things as remote access, internet usage, social media, email use, etc. In aggregate, these policies can be considered a building block for your firm's overall security program. Your security program should address people, process and policies. You may need help in developing your policies but their importance cannot be overstated..

The survey reported that 89% of respondents have one or more policies governing technology. Last year, the number was 83% and 77% in 2020. It is good news that implementations of policies are increasing over time.

As to specific policies, the *2022 Survey* reported that 67% have an email use policy followed by 63% with a computer acceptable use policy, 60% for internet use, 59% for remote access and 53% for disaster recovery/business continuity.

It is scary that only 42% of respondents reported as having an incident response plan. Larger firms, with much to lose, tend to be prepared with an incident response plan. As expected, firms of more than 100 attorneys are the most likely to have an incident response plan (72%), followed by 46% for firms of 10-49, 26% for firms of 2-9 and only 9% for solo respondents. There are many excuses for not having an incident response plan, but they don't negate your reason to have one. Think of your incident response plan as your "road map" for response and a plan for what needs to be done and who needs to do it. Without one, your firm will take on the characteristics of a headless chicken during a disaster or cyber incident.



## Security Defenses

What are attorneys doing to protect themselves from the apparent constant attacks? The *2022 Survey* gives us some insight into the various security tools law firms have available. Some sort of spam filter is the most common tool at 84%. Software firewalls was second at 79%, followed by mandatory passwords (74%), anti-spyware (73%) and email virus scanning (72%).

Encryption is a free or low cost solution to protect unauthorized access to data. To that end, the *2022 Survey* reported that 49% of respondents utilize file encryption. Email encryption is increasing. 40.1% of respondents indicated that email encryption was available. Law firms with 2-9 lawyers were at the low end with 30.4%. The percentage increased as the law firm size increased with 500 or more lawyers being at 53.3%. Larger law firms tend to have encrypted email as part of their email service, while the solo and small firm lawyers tend to take advantage of the secure communications capabilities within their practice management system.

## Security Assessments

One way to determine the firm's security posture is to perform an assessment. While performing periodic reviews of your own vulnerabilities, having a third party perform a security assessment can reveal more information using "fresh eyes" and cybersecurity scanning tools to survey your environment. Some cyber insurance carriers may require that a third party perform an assessment. Some clients may also want to know the status of your cybersecurity by requiring third party assessments or reviewing past assessments, policies and other documentation.

35% of respondents reported that their firms had a full security assessment performed by a third party. Respondents from firms of 2-9 lawyers reported 39%, 10-49 lawyers reported 30%, 50-99 lawyers reported 40% and 100-499 lawyers reported 53%. Solo lawyers were at the low end with only 14% responding that their firm had a security assessment conducted by a third party.

Besides having a third party perform a security assessment, 33% of respondents answered that a client or potential client had asked for the firm's security requirements document/guidelines. Larger firms are more likely to have a client or potential client request their security requirements document/guidelines with such a request being made to 57% of large firms over 100 lawyers, 33% for 50-99 lawyers, 38% for 10-49 lawyers and 20% for firms of 2-9 lawyers. Once again, solo lawyers were at the low end with only 5% of respondents stating that a client or potential client had asked for the firm's security requirements document/guidelines.

As mentioned earlier, some cyber insurance companies will require an assessment and/or completion of a questionnaire. The questionnaire answers are used to assess the risk to insure the law firm, thereby setting potential coverage limitations and rates. More and more clients are also interested in the security posture of their law firms. The *2022 Survey* reported that 30% of respondents answered that a client or potential client had asked their firm to complete a security questionnaire. Larger law firms are more likely to have a client or potential client ask their firm to complete a security questionnaire with 40% of firms over 100 lawyers answering in the affirmative followed by 20% of firms with 50-99 lawyers, 36% for 10-49 lawyers and 18% for firms of 2-9 lawyers. Solo attorneys were at 10%.

While some clients or potential clients requested completion of a questionnaire, fewer requested an actual security audit or other review of the firm's security. Only 12% of clients or potential clients requested such an audit or review.

## Cyber Insurance

Cyber liability coverage has been a white-hot topic over the last several years. Insurance premiums are increasing at a staggering rate. March McLennan Agency closely tracks cyber insurance trends. It identified ransomware and business interruption as the key drivers for the premium increases. In 2021, Marsh's

November Cyber Market Report indicated a 174% premium increase for the 12 month period ending in September 2021.

Despite the significant increase in premiums, 46% of respondents reported their firms having cyber liability insurance, which is up from 42% in 2021. Respondents from firms of 10-49 attorneys are the most likely to have cyber liability insurance (56%), followed by 43% of firms more than 100 attorneys, 42% firms of 2-9 attorneys, 40% firms of 50-99, and 38% for solo attorneys.

## Security Breaches

Probably the most quoted statistic from the *2021 Legal Technology Survey Report* was that 25% of respondents reported that their firms had experienced a data breach at some time. The *2022 Survey* asked respondents, "Has your firm ever experienced a security breach (e.g. lost/stolen computer or smartphone, hacker, break-in, website exploit)?" 27% of respondents answered in the affirmative. While the response appears to be a slight increase over last year, don't be misled in thinking over a quarter of law firms suffered a data breach. You may have lost your computer or smartphone or had it stolen, but that doesn't mean the data was accessible by unauthorized personnel or that the loss or theft constitutes a data breach. In other words, a security breach is not necessarily the same thing as a data breach.

Even though 27% experienced a security breach, 25% reported not knowing if their firm had ever experienced a security breach and 48% reported not having experienced one. The expectation would be for those in larger firms to be less knowledgeable about any security incident details. The results of the *2022 Survey* hold true to those expectations with the percentages increasing with firm size. The percentage of respondents who reported that they "don't know" is 5% for solo attorneys, followed by 12% for firms of 2-9 attorneys, 25% for firms of 10-49 attorneys, 33% for firms of 50-99 and 50% for firms of over 100.

## Prevention and Recovery

There were a few questions in the *2022 Survey* that addressed specific technologies. One technology was password management. Until such time as passwords are no longer required, we'll need to practice good password hygiene. This means no password reuse or the use of weak passwords. One tool to help with password management is a password manager. One survey question was "Do you use a password management tool (e.g. LastPass, Dashlane)?"

Overall, 32% of respondents reported that they use a password management tool, up from 31% last year. The responses were fairly flat across all firm sizes with 37% of respondents from firms over 100 attorneys reporting the usage of a password manager, followed by 34% for firms of 2-9 attorneys, 29% for solo attorneys, 26% for firms of 10-49 attorneys and 20% for firms of 50-99 attorneys.

Recovering data is extremely important to a law firm. With ransomware attacks increasing by leaps and bounds, having the ability to restore data is more important than ever. While the preference is to avoid a ransomware attack to begin with, having good backups is critical. The *2022 Survey* question was "How does your firm back up its computer files?" The most common response among all firms (29%) was that they use an Online backup such as Mozy, Carbonite, etc. The next most common response at 24% was Offsite (e.g. store backups at home, bank, other office), followed by External hard drive (21%) and Network attached storage (NAS) (20%). There are still some firms clinging on to legacy backup solutions such as tape and optical disc (CD & DVD).

No matter what backup technology you select, it should be engineered to survive a ransomware attack and be tested on a periodic basis. All the backups in the world won't do you any good if you can't restore the data. Performing test restores will give you confidence in your ability to recover from a cyber attack or natural disaster.

## Conclusion

This *TechReport* is a limited summary of what law firms are doing to address cybersecurity. Much more detail is available in the *Technology Basics & Security* volume of the *2022 American Bar Association Legal Technology Survey*. The good news is that law firms are improving their security posture, but more is still needed. New technologies utilizing advanced methods such as artificial intelligence and machine learning will provide even greater protection for the law firms of the future. While we can't predict a winner in the cyber wars, we can state it will be an ongoing battle. Attorneys need to constantly assess the security of their practices and evolve with the new threats and methods. Firms won't survive with a "set it and forget it" mentality. All law firms would be wise to heed the words of Benjamin Franklin when it comes to cybersecurity: "Failing to prepare is preparing to fail."

**ENTITY:**

**LEGAL TECHNOLOGY RESOURCE CENTER, LAW PRACTICE DIVISION**

**TOPIC:**

**PRACTICE MANAGEMENT, CYBERSECURITY, TECHNOLOGY**

## Authors

**John Simek**
Sensei Enterprises, Inc.

John Simek (jsimek@senseient.com) is the Vice President of Sensei Enterprises, Inc., a national managed IT service provider, digital forensics and managed cybersecurity firm located in Fairfax, VA. Mr. Simek has a national reputation as a digital forensics technologist and has testified as an expert witness throughout the United States. He holds a degree in engineering from the United States Merchant Marine Academy and an MBA in finance from Saint Joseph's University.