10 Things Every Lawyer Should Know About Cybersecurity in 2020

Webinar: March 31, 2020

1. Having a basic understanding of technology – including knowing the cyber risks of using the Internet, email and cloud computing – is not just a good idea, it's your ethical obligation.

ABA Model Rule of Professional Conduct 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] Maintaining Competence
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.

ABA Model Rule of Professional Conduct 1.4
An attorney must keep clients "reasonably informed" about the status of a matter and explain matters "to the extent reasonably necessary to permit a client to make an informed decision regarding the representation."

ABA Model Rule of Professional Conduct 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."

2. Here are the most common software threats that can infect your law office system.

Cyber attacks typically occur in one of the following ways, according to Law Crossing:

- Malware: Software that is intended to damage or disable computer systems or individual machines. It's a contraction of the words "malicious software," and it refers to things such as viruses, Trojan horses, spyware, etc.
- Ransomware: This type of malware locks down a computer and threatens to shut down the system unless a ransom is paid.
- Virus: Viruses are infected software that latch onto clean files and damage or corrupt them.
- Worms: A worm is a type of malware that replicates itself in order to spread to multiple computers. It is different from a virus in the fact that it can stand alone. A virus, on the other hand, needs to latch onto a host to work.

- Trojans: This type of malware discretely creates backdoors which allows hackers or other malware to enter your system. It was named after the Greek Trojan Horse, which refers to what appears to be a gift but is actually a deadly surprise.
- Spyware: Just as the name suggests, spyware is software used to spy on you. This includes recording your key strokes to learn your passwords or secretly using your camera to watch you.

Source: Law Crossing https://www.lawcrossing.com/employers/article/900048631/The-Importance-of-Cyber-Security-for-Law-Firms/

3. Twenty-six (26) percent of law firms have experienced a security breach, and another 19 percent may have experienced one but don't know it.

Adding those two figures together means a total of 45 percent of firms have experienced some sort of security breach, ranging from hacker activity and website exploits to less nefarious incidents like lost devices or stolen laptops, according to the 2019 ABA Legal Technology Survey.

"As might be expected, the larger the firm, the greater percentage of those unaware of whether their firms have ever experienced a breach (solo respondents, two percent; 2-9 lawyer firms, six percent; 10-49 lawyer firms, 24 percent; 100+ lawyer firms, 53 percent," the survey says. "Of course, there is no way to know the number of firms who don't yet know that they have been breached."

Thirty-six (36) percent of firms responding to the 2019 ABA Legal Technology Survey said their systems had been infected with viruses, spyware or malware in the prior year. The larger the firm, the greater the exposure, with 58 percent of firms with 100 or more lawyers reporting a viral, spyware or malware attack.

4. The consequences of a cyber attack can be catastrophic.

Consequences of a security incident:

- Consulting fees for repair (37 percent)
- Downtime/loss of billable hours (35 percent)
- Expense for replacing hardware or software (20 percent)
- Destruction or loss of files (15 percent)
- Notifying law enforcement of breach (9 percent)
- Notifying clients of the breach (9 percent)
- Unauthorized access to other (non-client) sensitive data (4 percent)
- Unauthorized access to sensitive client data (3 percent)

Consequences of a system attack:

- Destruction or loss of files (14 percent)
- Unauthorized access to (non-client) sensitive data (3 percent)
- Taking steps to report to law enforcement (1 percent)
- Taking steps to report to clients (1 percent)

Consequences of a virus, spyware, or malware infection:

- Costs incurred for consulting fees for repair (40 percent)
- Downtime/loss of billable hours (32 percent)
- Temporary loss of network access (23 percent)
- Temporary loss of web site access (17 percent)
- Replacement of hardware/software (15 percent)

Source: 2019 ABA Legal Technology Survey

5. Small businesses - including solo and small firms – are the most frequent targets of cyber attacks.

"Almost two-thirds of all cyber attacks are launched at small and mid-sized firms, according to this survey. And the average cost of a small business data breach is more than $85,000, says this report.

Law firms are especially tempting targets. Cyber thieves know firms have a trove of sensitive client data like financial records and Social Security Numbers. In addition, many firms have significant funds in the client trust account. Hackers also see law firms as conduits to larger fish like banks and corporations.

Many solo and small firms lack the budget, IT expertise and personnel required for a robust defense against cyber attacks.

In fact, more than half of small law firms and other businesses say they're worried about cyber threats but handicapped by cost limitations. When it comes to technology, they prefer tools that help with day-to-day operations, like computer accounting and data security programs.

Those are some of the findings from the MetLife & U.S. Chamber of Commerce Small Business Index, which surveyed small businesses about their attitudes towards technology adoption, cybersecurity, and data privacy.

According to the survey, the biggest factor holding small businesses back from adopting new technologies are:

- Cost (44 percent)
- The time it takes for IT training (25 percent)
- Lack of understanding of new technologies (19 percent)

Source: MetLife & U.S. Chamber of Commerce Small Business Index

6. Email phishing scams are growing more sophisticated by the day.

More than 90 percent of viruses, malware and ransomware are transmitted by way of a phishing email.

If you get an email that says "Password Check Required Immediately," open it at your peril. It's the most common phishing email subject line used by scammers, according to the cyber-security site KnowBe4.

The next most popular scam lines: "A Delivery Attempt Was Made," "Deactivation of Your Email Is in Progress," and "New Food Trucks Coming to [Your Company's Location]."

Top 10 General Email Phishing Lines

1. Password Check Required Immediately
2. A Delivery Attempt Was Made
3. Deactivation of Your Email Is in Progress
4. New Food Trucks Coming to [Your Company's Location]
5. Updated Employee Benefits
6. Revised Vacation and Sick Time Policy
7. You Have a New Voicemail
8. Organizational Changes
9. Change of Password Required Immediately
10. Staff Review 2018

Source: KnowBe4

7. Eleven Ways to protect yourself from a cyber attack:

1. Train and educate your staff to recognize, report and respond appropriately to a cyber threat or cyber event.
2. Make sure all software programs are up-to-date and functioning properly.
3. Install updates and patches when they become available.
4. Use secure passwords (a password manager is recommended) and change them often.
5. Use two-factor authentication.
6. Have an office policy on cyber preparedness.
7. Make sure your office policy has clear guidelines for working remotely and taking laptops and devices off-site.
8. Limit access to sensitive systems, files and data.
9. Obtain cyber liability insurance.
10. Discuss ABA Model Rule 1.1 and its ramifications at your next office staff meeting.
11. Have an Incident Response Plan.

8. Last year, US businesses – including law firms – lost $1.5 billion to wire fraud.

In 2015, a total of $220 million was lost in the US to wire fraud. Last year, that figure skyrocketed to $1.5 billion – most of it done via email, according to WFG National Title Insurance Co. The reason for this alarming rise: cyber criminals are getting more sophisticated with social engineering scams by the day.

The big takeaway: If you are instructed by email to transfer money, call the individual or business who purportedly sent the email and confirm that the request is legitimate.

9. Your firm should develop an Incident Response plan.

In 2019, a total of 31 percent of law firms had a formal Incident Response Plan, up from just 25 percent of firms the year before, according to the 2019 ABA Legal Technology Report.

The breakdown of Incident Response Plans according to firm size: solos (11 percent); firms with 2-9 attorneys (23 percent); firms of 10-49 (35 percent); firms with 100+ attorneys dipped (65 percent).

Key elements of an Incident Response Plan:

- Procedures for initial reporting of an incident
- Confirmation of the incident
- Escalation as appropriate
- Investigation
- Having a designated incident response project manager
- Assembling a cross-disciplinary response team
- Training the response team on breach reporting obligations, mitigation requirements and the steps needed for recovery. The team might include everyone from IT professionals to a PR firm.
- Post-incident review
- Revising the plan to incorporate all lessons learned
-

Pro Tip #1: Make sure your Incident Response Plan complies with applicable laws, professional obligations and standards set out by The National Institute of Standards and Technology (NIST).

Pro Tip #2: Review ABA Ethics Opinion 483 for consideration of ethical issues that might be implicated in a cyber incident.
Source: 2019 ABA Legal Technology Report

10. The number of law firms that have obtained cyber liability insurance has tripled (to 36 percent) in the past five years, according to the first-ever ABA Profile of the Legal Profession.

In 2015, only 11 percent of firms with two to nine lawyers had cyber liability coverage, according to the ABA Profile of the Legal Profession survey. That percentage soared to 36 percent in 2018. For firms with 10 to 49 attorneys, the increase was just as dramatic. In 2015, only 15 percent of those firms had cyber coverage. In 2018, the percentage was 47 percent.

Lawyers Whose Firm Has Ever Experienced a Data Breach

- **2018**: Solo firms (14 percent); 2-9 lawyers (24 percent); 10-49 lawyers (25 percent); 100-499 lawyers (31 percent); 500 or more (31 percent)
- **2017**: Solo firms (11 percent); 2-9 lawyers (27 percent); 10-49 lawyers (35 percent); 100-499 lawyers (17 percent); 500 or more (23 percent)
- **2016**: Solo firms (8 percent); 2-9 lawyers (11 percent); 10-49 lawyers (25 percent); 100-499 lawyers (16 percent); 500 or more (26 percent)

- **2015**: Solo firms (11 percent); 2-9 lawyers (16 percent); 10-49 lawyers (14 percent); 100-499 lawyers (23 percent); 500 or more (23 percent)

Law Firms with Cyber Liability Insurance

- **2018**: Solo firms (27 percent); 2-9 lawyers (36 percent); 10-49 lawyers (47 percent); 100-499 lawyers (38 percent); 500 or more (31 percent)
- **2017**: Solo firms (19 percent); 2-9 lawyers (27 percent); 10-49 lawyers (35 percent); 100-499 lawyers (34 percent); 500 or more (27 percent)
- **2016**: Solo firms (16 percent); 2-9 lawyers (17 percent); 10-49 lawyers (22 percent); 100-499 lawyers (20 percent); 500 or more (14 percent)
- **2015**: Solo firms (10 percent); 2-9 lawyers (11 percent); 10-49 lawyers (15 percent); 100-499 lawyers (11 percent); 500 or more (13 percent)

Source: ABA Profile of the Legal Profession survey

ABOUT THE SPEAKERS AND MODERATOR

Kevin M. O'Hagan, JD
Kevin O'Hagan is a founding partner of O'Hagan Meyer. After practicing at large law firms for 15 years, such as McGuire Woods and Locke Lord Edwards, he founded the firm to be a national boutique with an emphasis on personal customer service. He acts as lead counsel for several Fortune 500 companies and has tried cases in five different states, including the Delaware Court of Chancery, and has mediated cases in 15 state courts and federal jurisdictions. Kevin has also handled multi-district litigation and class action suits. He is licensed to practice in Illinois and Virginia, and has been admitted to practice *pro hac vice* in 10 other states. *Chicago Lawyer* Magazine, in its inaugural annual edition, recognized Kevin as one of the city's *Top 40 Lawyers under 40 to Watch* and he was named a *SuperLawyer* by *Chicago Magazine* in 2005, and 2008-2021. Kevin is National Chair of the Firm's Director's & Officers practice and has successfully handled shareholder, intellectual property, restrictive covenant and breach of fiduciary matters all over the country.

Jamey Davidson, JD. Jamey Davidson is a partner in the Chicago office of O'Hagan Meyer. He heads the Chicago Office's Cyber Liability and Data Privacy Practice Group. Jamey represents insurance companies as well as their insureds in Cyber Liability matters ranging from ransomware matters to cybercrime matters. He acts as Breach Coach and Privacy Counsel to large and small companies responding to cyberattacks and cyber threats. He acts as monitoring counsel for domestic and London based cyber liability carriers for matters all over the country and has successfully negotiated many ransom and extortion payments and worked to recover funds that were stolen in cybercrime schemes. Jamey frequently writes and lectures on cyber liability, cyber liability insurance issues, the ethical issues and legal responsibilities of lawyers, damages in legal malpractice actions, attorney-client privilege and client confidentiality.

Moderator
Ernest (Jay) Reeves Jr. has worked in the legal profession for more than 40 years, including 35 years of private practice in North Carolina and South Carolina (where he represented lawyers in licensing, ethics and bar disciplinary matters). He has also been Legal Editor at Lawyers Weekly and Vice President of Risk Management at Lawyers Mutual of NC.

He has presented hundreds of CLE programs to lawyers and bar groups on practice management, ethics and tech topics, including the 10 Building Blocks of Risk Management, which he has presented across the U.S. and Canada. He was a panelist and moderator for the recent CLE webinars "Law Firm Cybersecurity Best Practices 2021" and "Putting Cybersecurity to Work in Your Practice," both of which were CLE-accredited in multiple states.

He helped launch the North Carolina Legal Tech Expo in the late 1990s, a trail-blazing immersive tech experience for lawyers sponsored by the NC Bar Association. He was a past Vice-President of BarCARES of North Carolina. He was a member of the Orange County (NC) Bar Professionalism Oath Committee. He is author of the book, "*The Most Powerful Attorney in the World*." He is founder and owner of Your Law Life LLC. He now runs Your Law Life LLC, which helps lawyers and firms stay safe and successful.

Contact: Jay Reeves, Your Law Life LLC
Phone 919-619-2441
jay@yourlawlife.com

SPONSOR
Alta Pro Insurance Services
Lawyers Risk Purchasing Group

www.altaprorpg.com info@altaprolawyersrpg.com

DISCLAIMER: This manuscript contains general information that might be helpful in your practice. It addresses risk management and ethical considerations regarding technology and cybersecurity. Nothing in this manuscript is intended as legal advice or opinion, nor is this manuscript intended to establish the legal standard of care applicable to any situation. Each case is different, and each client has different needs. The law changes rapidly. Independent research and due diligence are always part of your ethical responsibility.