Cybersecurity Ethics
Safeguarding Client Data in Today's Emerging Hybrid Practice

Thursday, June 29, 2022
12 Noon – 1:00 PM CST
Live, online webinar

Presenter
David G. Ries, Attorney
Of counsel, Clark Hill PLC (Pittsburgh, PA)
dries@clarkhill.com
(Author of Cybersecurity section of 2021 ABA TechReport; co-author, *Encryption Made Simple for Lawyers* (ABA 2015) and *Locked Down: Practical Information Security for Lawyers* (ABA 2016)

Moderator: Jay Reeves, JD
Your Law Life LLC, Chapel Hill, NC
jay@yourlawlife.com

Introduction

The pandemic transformed the legal profession in ways that were unimaginable not long ago. The 2021 ABA Legal Technology Report shows just how dramatic that change has been.

The presenter of this webinar, David G. Ries, is a national thought leader in the burgeoning field of Cybersecurity Ethics. He is author of the Cybersecurity Chapter for the ABA TechReport 2021 and the book *Locked Down: Practical Information Security for Lawyers* (ABA 2016). In this webinar, Ries will examine surveys, statistics and trends data of the 2021 ABA TechReport to extract valuable pointers for keeping your practice safe, ethical and successful.

Attendees will learn how technology and cybersecurity affect their ethical obligations, including compliance with the Rules of Professional Conduct. They will discover best practices for safeguarding client data, maintaining technological competence, and running a virtual law practice. And they will learn how to put Cybersecurity Ethics into practice to protect their firms, clients and data.

Part One
Recognizing the Threats

Cyberthreats to attorneys and law firms are at an all-time high and continue to grow. The pandemic brought new threats and risks as law firms relied on tech in pivoting to online conferencing, remote work, cloud computing and virtual practice.

The 2021 ABA TechReport found that 17 percent of solos and small firms (2-9 lawyers) experienced a data breach in 2021; 35 percent of firms with 10-49 lawyers; 46 percent with 50-99 lawyers; and about 35 percent with 100+.

Highlighting the risk, ABA Formal Opinion 483 says: "[T]he data security threat is so high that law enforcement officials regularly divide business entities into two categories: those that have been hacked and those that will be." [*Source: ABA Formal Ethics Opinion 483*]

Cyberthreats are a particular concern for attorneys because of their duty to safeguard client property and maintain confidentiality. This session will explore current threats – paying special attention to scams and schemes that target law firms – and practical ways to comply with your professional responsibilities in today's emerging hybrid practice.

- Why attorneys and law firms are targets
- Dangers of hybrid and remote practice
- Today's greatest threats
    - Ransomware
    - Spearphishing
    - Business email compromise
    - Lost and stolen laptops, smartphones and portable devices

A starting point for prevention is to conduct an in-firm audit/risk assessment to identify your firm's strengths, needs, and unique vulnerabilities. The audit should cover personnel, hardware, software, vendor agreements, and office policies and procedures.

In deciding what tech tools are right for your firm, Comment [18] to ABA Model Rule 1.6 suggests weighing "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)."

Part Two
Ethical Duty to Safeguard Data

Lawyers are increasingly facing professional consequences – including bar discipline – if their clients are damaged because of a cyber breach or technology incompetence. Example: the North Carolina State Bar recently notified lawyers who handle entrusted funds they are under a "heightened duty" to safeguard against email wire transfer fraud.

ABA Model Rule 1.1(8) Competence: "To maintain 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***."

This session will explore key professional and ethical obligations – from common law to the Model Rules of Professional Conduct – related to technology and cybersecurity.

Important Cyber/Tech Ethics Rules and Opinions

- ABA Model Rule 1.4 (Communication), Rule 1.6 (Confidentiality) and Rules 5.1 - 5.3 Supervision)
- ABA Formal Opinion 498 Virtual Practice (Feb 2021)

- ABA Formal Opinion 477R Securing Communication of Protected Client Information (May 2017)
- ABA Formal Opinion 483 Lawyers' Obligations After an Electronic Data Breach or Cyberattack (October 2018)

"Together, these rules require attorneys, when using technology, to 1) employ competent and reasonable measures to safeguard the confidentiality of information relating to clients, 2) communicate with clients about the attorneys' use of technology and obtain informed consent from clients when appropriate, and 3) to supervise subordinate attorneys, law firm staff, and service providers to make sure that they comply with these duties." [*Source: 2021 ABA TechReport: Cybersecurity, by David Ries]*

Professional obligations re technology and cybersecurity may also arise through:

- Common law
- Contracts
- Laws and regulation

Part Three
Cybersecurity 101 for Your Firm

A little more than half of law firms (53 percent) have a formal policy for managing and safeguarding data and information, according to the 2021 ABA TechReport. That number has risen steadily over time.

The ABA "encourages all private and public sector organizations [law firms included] 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." [*Source: ABA Report and Resolution 109*]

An effective cybersecurity program should be tailored to the specifics of your law practice. The program should cover People, Procedures and Technology.

"Security should not be left solely to IT staff and tech consultants," writes Ries in the 2021 ABA TechReport. "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 security incidents and data breaches. Cybersecurity programs should cover all of these functions."

- Comprehensive cybersecurity program
- Standards and frameworks
- Manage and minimize data
- Incident response plan (*36 percent of firms of all sizes have some sort of response plan, per the 2021 ABA TechReport*)

Here are some law office technology usage statistics from the *2021 Survey:*

- 53 percent of responding firms have a data retention policy

- 60 percent have a policy on email use
- 56 percent for internet use
- 57 percent for computer acceptable use
- 56 percent for remote access
- 48 percent for social media
- 32 percent personal technology use/BYOD
- 44 percent for employee privacy

Twenty-five (25) percent of firms said they either had no cybersecurity policies in their office or did not know whether they had any.

Part Four
Putting Cybersecurity Ethics into Action

1) Practical Lessons from ABA TECHREPORT Cybersecurity 2021

Covering all bases from websites to working from home.

2) Ten Basic Safeguards for your practice

(Source: "Safeguarding Client Data – Addressing Cybersecurity Basics," *Law Practice Magazine;* May-June 2022)

3) Most Widely Used Law Firm Cybersecurity Tools

- Spam filter (81 percent; this may be under-reported because most email service providers have at least basic spam filters)
- Software-based firewalls (75 percent)
- Anti-spyware (75 percent)
- Mandatory passwords (70 percent)
- Antivirus for desktops/laptops as well as for e-mail (both about 70 percent)
- Intrusion detection and prevention systems (33 percent)

[*Source: 2021 ABA TechReport*]

4) Third-Party Security Assessments / Client Security Requirements

"Clients are increasingly focusing on the cybersecurity of law firms representing them and using approaches like required third-party security assessments, security requirements, and questionnaires," writes Ries in the report. "The increased use of security assessments conducted by independent third parties has been a growing security practice. Law firms have been slow to adopt this security tool, with only 27 percent of law firms overall reporting that they had a full assessment. Affirmative responses generally increase with the size of the firm. Overall, 30 percent of respondents report that they have received a client security requirements document or guidelines, with affirmative responses generally increasing by firm size."

5) Cyber Insurance

Forty-two (42) percent of attorneys have cyber liability coverage, according to the TechReport. That percentage has been increasing in recent years. From Ries: "A review of the need for cyber insurance coverage should be a part of the risk assessment process for law firms of all sizes."

6) Passwords and access controls. This is the first line of defense for your firm. Seventy (70) percent of firms overall say they use mandatory passwords [50 percent of solos, 73 percent of 2-10 lawyer firms; 80 percent or higher for large firms. Eleven (11) percent of firms use biometric login.

7) Multifactor authentication. MFA uses two or three of the following factors: (a) something the user knows ex: a password); (b) something the user has (ex: a security app on a smartphone); (c) something the user is (ex: a fingerprint or face scan).

8) Avoid "Bad Practices." The Cybsersecurity & Infrastructure Security Agency (CISA) publishes a catalog of Bad Practices that are exceptionally risky. Three bad practices are:

- Using single-factor authentication
- Using unsupported or "end-of-life" software
- Using weak or default passwords and credentials

[*Source: CISA*]

ABOUT THE SPEAKER AND MODERATOR

David G. Ries is of counsel in the Pittsburgh, PA office of Clark Hill PLC, where he practices in the areas of technology, data protection, and environmental law and litigation. David served on the ABA Cybersecurity Legal Task Force and the ABA TECHSHOW Planning Board. He is author of the Cybersecurity Section of the 2021 ABA Legal Technology Survey Report.

David is a coauthor of *Locked Down: Practical Information Security for Lawyers, Second Ed.* (American Bar Association 2016) and *Encryption Made Simple for Lawyers* (American Bar Association 2015) and a contributing author to *Information Security and Privacy: A Legal, Business and Technical Handbook, Second Edition* (American Bar Association 2011).

For more than 25 years, he has focused on cybersecurity law, privacy, technology, data protection challenges, and information governance. He has used computers in his practice since the early 1980s and since then has strongly encouraged attorneys to embrace technology – in appropriate and secure ways.

Dave speaks and writes nationally on legal ethics, technology, and cybersecurity topics. In May 2022, he presented a talk on "Cybersecurity Ethics" at the ABA Law Practice Division's Spring Meeting.

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.