Alta Pro Risk Purchasing Group (RPG)

The Cyberthreat Landscape for Law Firms
2023 Mid-Year Report

Live webinar July 13, 2023
12 Noon CST
1.0 Hour CLE Webinar

Presenters
James Davidson, O'Hagan Meyer Attorneys & Advisors
Jay Reeves, JD (Your Law Life LLC)

INTRODUCTION

As we approach the midpoint of 2023, the cyberthreat landscape for law firms remains in some ways unchanged since the year began. The same culprits – human error, lack of team training, social manipulation – cause the most problems.

But in other ways, things have grown worse. New and more insidious threats emerge each day. Increasing reliance on cloud technologies and remote servers for data storage is heightening the risk of a cyber attack or data breach.

Meanwhile, lawyers have an ethical obligation (Rule 1.1) to stay current on changes in technology and cybersecurity.

This program will help attorneys and legal professionals comply with Rule 1.1 by exploring the mid-year cyber landscape and taking a deep dive into attorney ethics and best practices.

CONTENTS

1. Rule 1.1 Ethical Duty of Technological Competence

ABA Model Rule of Professional Conduct 1.1 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 ...."*

How much IT are you expected to know? How thoroughly should you vet a cloud computing tech vendor? Can you just hire others to do these things for you?

The answers are unclear. Rule 1.1 Comment 8 is evolving, as technology is evolving.

"The rapidly approaching threat to job security is that lawyers who aren't technically savvy will be replaced by those who are," says this article in the ABA Journal.

2. ABA Adopts First-ever Guidelines for AI Usage

For the first time, the American Bar Association has passed a Resolution establishing guardrails and guidelines for using AI technology.

ABA Resolution 604 was adopted at the 2023 Midyear Meeting of the American Bar Association. Three main points:

1. *Developers of AI should ensure their products, services, systems and capabilities are subject to human authority, oversight and control.*
2. *Organizations should be accountable for consequences related to their use of AI, including any legally cognizable injury or harm caused by their actions, unless they have taken reasonable steps to prevent harm or injury.*
3. *Developers should ensure the transparency and traceability of their AI and protect related intellectual property by documenting key decisions made regarding the design and risk of data sets, procedures and outcomes underlying their AI.*

Here is a "Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People" released in October 2022.

Here is an initiative launched in 2021 by the US Equal Employment Security Commission to prevent discrimination in AI contexts.

ABA Resolution 112 "urged lawyers and courts to address ethical and legal issues arising from the use of AI in the practice of law." ABA Resolution 700 "called on governmental entities to refrain from using pretrial risk-assessment tools unless 'the data supporting the risk assessment is transparent, publicly disclosed and validated to demonstrate the absence of conscious or unconscious racial, ethnic or other demographic, geographic or socioeconomic bias."

3. Top Cyber Threats

A new cybersecurity report shows email phishing scams are the most common form of attack. Among the global businesses surveyed, the following have experienced a cyber incident in the past 12 months:

- Email Phishing attack – 81%
- Network attack – 66%
- Application attack – 56%
- Cloud attack – 56%
- Device/Endpoint attack – 55%
- Ransomware attack – 53%
- Supply Chain attack – 50%

SOURCE: KnowBe4 Blog
Phishing Tops the List Globally as Both Initial Attack Vector and as part of Cyberattacks (knowbe4.com)

4. Emerging Risks

A) Typosquatting and combosquatting
Typosquatting is sometimes referred to as URL hijacking. It relies on a mistake by the user (ex: making a simple typo when entering a URL) to direct them to a bogus site or get them to divulge sensitive data.

Combosquatting is when a fake domain is created that appears real because it contains words or phrases of legitimate businesses, but bogus words or characters have been added. The site is of course a trap for the unwary.

B. Government Imposter Scams
Scams involving fake Social Security and Medicare communications spike during annual enrollment periods and tax season.

One red flag: receiving an "official" text or letter from the Social Security Administration that you were not expecting. The SSA notice may arrive by email, regular mail, social media, telephone or text.

C) W-2 Phishing Scams
In the W-2 email spoof, a recipient receives a link to access their tax forms online.

"Malicious actors routinely target human resources professionals, certified public accountants, and individual employees with social engineering attacks during tax season in an effort to obtain copies of Internal Revenue Service Form W-2 (Wage and Tax Statement)," says attorney Alyssa Watzman for Constagny Law Firm Cyber Team. "Form W-2 contains the information that allows a malicious actor to file false tax returns and steal the refunds." Read "Social Engineering in Tax Season: Form W-2 Exploits" here.

5. Zero-Trust Cyber Security for your Law Practice

When it comes to law firm cybersecurity, "trust, but verify" is a good approach.

A "zero trust" mindset is even better.

Although the term "zero trust" – also called zero trust architecture, zero trust network access, or perimiterless security – has been bouncing around the IT world since the 1990s. But only recently has it entered the mainstream.

"Trust, but verify" is like locking the front door to your law office. Nobody gets in until they are verified, but once they're in, they can wander around the entire office – the lobby, computer room, and break room. Under a "zero trust" philosophy, nobody gets in until verified. But once in, they are restricted as to what rooms they can enter and what they can do once inside.

Zero trust starts with an assumption that every connection and endpoint is a threat and operates on the principle of least privilege (PoLP).

Read "What is Zero Trust?" in the US Chamber of Commerce newsletter CO.
Read "5 Core Principles of Zero Trust" in Forbes.

6. Small Business Data Breach Case Studies

FRAUDULENT FUNDS TRANSFER LOSS
Description. An administrative assistant at a real estate agency received an e-mail purporting to be from the CEO of the agency, asking that $275,000.00 be wired from the agency's account for a closing for a new home. The e-mail address was the actual address of the CEO. The assistant responded and had the funds wired as instructed. The wire instructions were fraudulent. This fraud was the result of an e-mail breach wherein the hacker had access to the CEO's e-mail account and set up a folder that only the hacker could see.

Losses:
Fraudulent Funds Transfer Loss - $275,000.00
Forensic IT analysis of E-mail Breach - $27,500.00

OFFICE 365 DATA BREACH
Description. A small accounting firm had its e-mail system breached via a phishing e-mail that allowed the hacker to have access to an assistant's e-mail account and Office 365 account. The accounting firm handled many private client tax returns and exchanged financial information and draft returns via unencrypted messages. A review of the assistant's Outlook account revealed that the hacker had access to the account for a period of 14 days during tax season.

Losses:
Privacy Counsel - $40,000.00
Data Breach Expenses - $30,000.00
Notification Cost: $10,000.00
Credit Monitoring Costs: $10,000.00

WEBSITE VIRUS

Description. A financial management firm had a virus infect its system wherein any e-mail that contained a link to the company's website was blocked by the recipient's spam filter. The virus was only for the purpose of causing mayhem and chaos. The firm lost clients and had to notify all receipts of the e-mails that did not get caught by a spam filter that if they opened the e-mail, the virus could have affected their computer or system. There is the potential for resultant third-party claims if the recipients' systems were damaged.

Losses:
Data Breach Expenses - $40,000.00
Notification Costs - $5,000.00

EMPLOYEE LOST AND STOLEN LAPTOP AND MOBILE PHONE
Description. A mid-sized office supply company performed month-end financial reports which included customer information, account information, financial information and information regarding bank accounts and wire information. The information was distributed to several employees, one of which had a personal laptop and mobile phone stolen. In conjunction with IT, but without discussing with the company, the employee was given access to e-mail on his personal laptop and mobile phone. Neither of which required multi-factor identification, no encryption and ability to bypass passwords if sessions were active.

Losses:
Privacy Counsel - $45,000.00
Notification Costs - $20,000.00
Credit Monitoring - $30,000.00

(Source: O'Hagan Meyer)

7. Best Practices for Law Firms

- **Develop a Cyber Policy.** Educate and train your employees. Conduct periodic refresher training.
- **Have a Specific Policy for Wiring Funds or Sending Money.** For law firms and any business that routinely wires funds, a policy of verifying the instructions via a phone call should be mandatory for anything over a small amount (i.e. $1,000.00). Further, an instruction on an e-mail to clients that they should call and verify any change in payment/wire instructions they receive should be made. Further, if you're depositing a large check in a Trust Account with the funds to then be wired out, require that the funds actually clear before they leave the Trust Account.
- **PICK UP THE PHONE AND CALL BEFORE WIRING FUNDS**
- **Have a Specific Policy about Opening Links from Unknown Sources.** First verify the e-mail is legitimate or show it to IT. No employee should ever provide credentials such as a password or username in such an instance.
- **Have a Personal Use Internet Policy.** Or enforce the policy you already have.
- **Have a Cell Phone and Personal Computer Policy.** Devices should be vetted and approved by the company's IT.
- **Have a Combination of Firewalls and Data Encryption.** A multi-level defense is best.
- **Have your IT Explain its Back-Up Procedures.** Run tests on your system

- **Make Sure all Virus and Anti-Malware Software is up to Date.** Follow-up as needed.
- **Have a Password Policy.** More than half of data breaches are caused by weak or nonexistent passwords.
- **Back Up Cloud Data.** Cloud backups should be secured with MFA and regularly tested at a rate of more than once per day.
- **Consider Annual Penetration Testing.** Many forensic IT companies offer services where the company network and e-mail are tested to highlight vulnerabilities and then offer solutions to "close the holes."

(Source: O'Hagan Meyer)

ABOUT THE SPEAKERS

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.

Jay Reeves, JD. Jay is the Risk Pro for Alta Pro Insurance Services. He practiced law in South Carolina and North Carolina for nearly 40 years, both in private practice and in-house (as corporate VP/Risk Manager for Lawyers Mutual Liability Insurance Company of North Carolina). His practice concentrated in representing attorneys in ethics, licensing and disciplinary cases. He has given more than 250 presentations on legal ethics and professionalism to bar groups, law firms and law schools in the U.S. and Canada. He is founder and owner of Your Law Life LLC. He is author of the law column "Ask the Risk Man" and the book "The Most Powerful Attorney in the World."

Contact:
jay@yourlawlife.com
Ph: 919-619-2441
www.yourlawlife.com