Risk Management in Cyberia: Safeguarding Client and Law Firm Information

ALA Right Now: A Virtual Conference
December 8, 2020

1

Recent Headlines

More Than 100 Law Firms Have Reported Data Breaches. And the Problem Is Getting Worse | Law.com

Security, Privacy Crucial To Working From Home, Pa. Bar Says

Law Firms Remain Vulnerable to Wire Transfer Scams, as Liability and Breach Costs Grow

Battling Bad Actors: Law Firms Must Fight Cyber Threats with Culture Change

2

2

Why Are Lawyers At Risk?

Lawyers sling millions of gigabytes of confidential information daily through cyberspace, conducting much of their business via email or smartphones and other mobile devices that provide ready access to documents. But the new tools also offer tempting targets for hackers, who experts say regard law firms as "soft targets" in their hunt for insider scoops on mergers, patents and other deals.

Wall Street Journal, June 25, 2012

3

3

Program Agenda

1 The Current Threat Landscape for Law Firms

2 Sources of Lawyers' Obligations to Protect Client and Law Firm Information

4

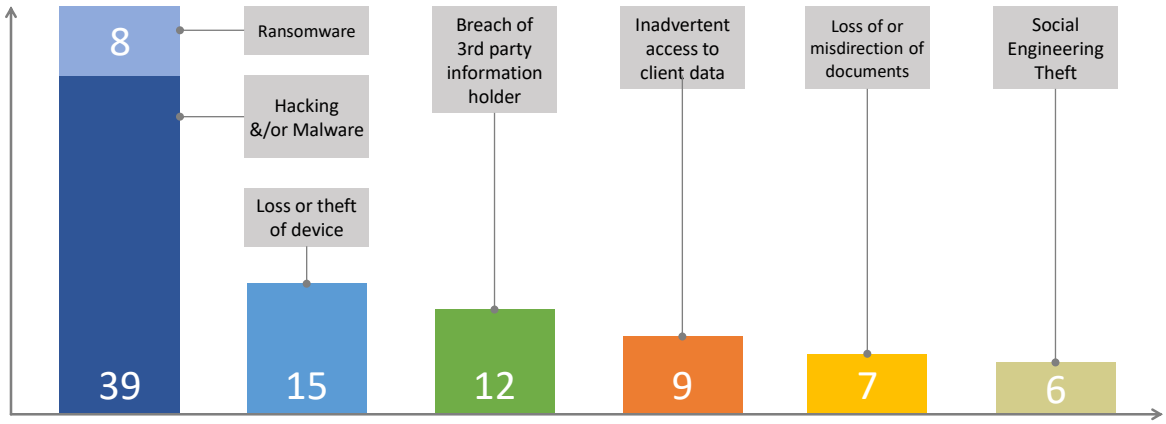
4

The External Threat Landscape

5

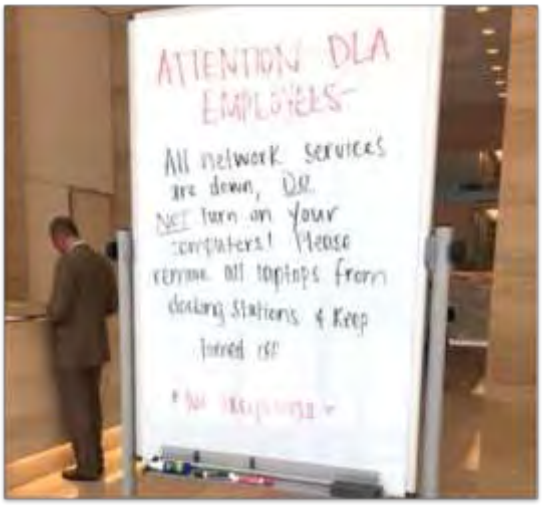
Aon Professional Services Firm Cyber Events

88 matters recorded since 2009



6

Malware – Ransomware



7

7

Ransomware 2.0

After targeting two **law firms** in the past couple of months, a hacker group called **Maze** has struck the **legal** industry again, publicizing a **ransomware** attack on three **small** South Dakota **firms** and vowing to publicly publish their confidential data if the **firms** do not pay up. Feb 4, 2020

Lady Gaga's Law Firm Got Hacked. Now What?

Allen Grubman's New York firm says its celebrity clients have shown "overwhelming support" despite a multimillion-dollar ransomware demand. But do entertainment boutiques face special risks, both before and after an attack?

By **David Thomas** May 18, 2020 at 01:58 PM

8

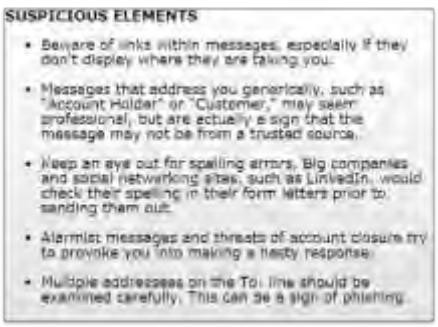
8

Third Party Vendors

9

9

Phishing Emails



10

10

The Phishing Attacks Keep Getting Better …

"Trusted Source

- Co-worker, supervisor, firm leadership
- LinkedIn
- U.S. Postal Service, Amazon, Fed Ex

Urgent Message

- Wire Transfer Assistance
- W-2 Requests
- DocuSign
- Account Suspended/Fraudulent Activity

Recognition or Award

Phishing Attacks – Best Practices

- Never open a link or attachment sent via email unless you are expecting the communication and know the sender and the context of the request.
- Never reply to an unexpected email message asking if the link or attachment is legitimate—even if you know the sender.
- Never ask your co-worker to help you try to open an email attachment or check a link shared with you.
- Always report suspicious emails, activities, or requests to the firm's IT department, designated individual, or general counsel.

Don’t Forget About Fake Client Scams

Hello My Dearest,

Nadia Kone [user5@badg.cc]

Hello My Dearest,

How are you today,I hope this message will find you in the best of your health, I really like to have a good relationship with you, and I have a special reason why I decided to contact you because of the urgency of my situation here.

Please I write not only to introduce myself to you, but also tender a joint investment business proposal for your considerations and acceptance. I know that receipt of my communication shall be a great surprise to you considering the fact that we do not know each other or had any business negotiations before now,I am also aware of the fact that there is a lot of fraudulent business proposals circulating around the world, mostly from African continent, which makes it imperative for one to be extremely careful before accepting and venturing any business proposal from unfamiliar person like me.

I however, pray your respected self not to allow the above unnatural abnormalities to influence your decision to accept my genuine proposal and intentions which undoubtedly would be of immence mutual benefits to both of us. I pledge to you for urgent and dedicated attention which this issue deserves.

13

13

Don’t Forget About Fake Client Scams

14

14

An Actual Nigerian Scam Victim

- An Iowa lawyer's lucky client due to inherit $18.8 million.
- Client had to pay $177,660 in Nigerian inheritance taxes and additional cash for an "anti-terrorism certificate" before receiving the money.
- Lawyer charged a 10% contingency fee to secure the inheritance
- Iowa lawyer solicited more than $200,000 in loans from five current and former clients, promising to quadruple their investment once the inheritance was obtained
- The Iowa Supreme Court Disciplinary Board concluded that the lawyer "appears to have honestly believed—and continues to believe—that one day a trunk full of ... one hundred dollar bills is going to appear upon his office doorstep"

15

15

Fake Client Email Scams – Detection Tips

- Generic greeting or unsolicited requests
- Incorrect grammar or poor spelling
- Urgent action required
- Outside your area of expertise
- Lack of specifics ("your jurisdiction")
- Google the client name or unusual legal terminology
- Email is from a foreign country
- Requested service is to collect or receive money and then transfer it to someone you have never met

16

16

Wire Transfer Scams

Holland & Knight Sued Over Botched Wire Transfer

Law360 (May 21, 2020, 4:24 PM EDT) -- A Boston law firm targeted by an email scam can't hold First Republic Bank responsible for processing a $237,000 counterfeit check and subsequent wire transfers because the bank was simply following the firm's directions, the Massachusetts intermediate-level appeals court ruled Wednesday.

Law Firm Can't Blame First Republic For $300K Email Scam

By Rachel Sharp

Law360 (May 21, 2020, 4:24 PM EDT) -- A Boston law firm targeted by an email scam can't hold First Republic Bank responsible for processing a $237,000 counterfeit check and subsequent wire transfers because the bank was simply following the firm's directions, the Massachusetts intermediate-level appeals court ruled Wednesday.

Law Firm Can't Sue Citigroup After Email Hack Heist

By Ben Kochman

Law360 (April 27, 2020, 6:16 PM EDT) -- A Washington, D.C., law firm can't sue Citigroup Inc. after a thief allegedly hacked into the firm's managing partner's email and diverted $60,000 meant for the firm into a Citibank account, because it has not shown the bank knew about or helped with the crime, a D.C. federal judge said.

Wire Transfer Best Practices

- Authenticate all wire transfer requests by telephone or in person.
  - Use the telephone number on file or independently look up the number.
  - Do not use the number contained in the requesting party's email.
- Where feasible, have two parties to a transaction make the wire transfer request. Dual authorization increases the likelihood of authenticity.
- Be particularly suspicious of wire transfer requests that deviate from previously agreed arrangements.
- Carefully review requests for unusual grammar usage and misspellings.
- Review the account beneficiary listed on the wire transfer instruction and the recipient bank for any oddities.

The Internal Threat Landscape

19

19

Simple Carelessness – Hall of Fame Candidates

- A Maryland law firm lost an unencrypted portable hard drive that contained medical records of patients in a lawsuit against its client hospital.
  - One of the law firm's employees took home the hard drive containing backup data. This was the firm's method of ensuring that it had an off-site backup. She took the light rail system home and left the drive on the train. When she came back a few minutes later, it was gone.
- In July 2008, sheriff's deputies uncovered hundreds of people's personal financial files held by a Houston law firm that had been discarded in a dumpster.

20

20

Malicious Insiders

- On April 16, 2016, a former IT manager of Locke Lord LLP was sentenced to 9 years in prison and fined $1.7 million for a destructive computer attack he committed against the Dallas law firm in 2011.
  - Four months after his employment ended, the individual accessed Locke Lord's systems and issued commands that caused "significant damage" to the network, "including deleting or disabling hundreds of user accounts, desktop and laptop accounts, and user e-mail accounts."
- In 2011, a fired employee of a Pittsburgh, PA based law firm used his old computer credentials to give members of the protest group "Anonymous" access to the firm's systems. The group erased all of the firm's files and backup files.

21

21

Insider Trading

- In May 2017, the U.S. government charged a former BigLaw partner with trading stock ahead of major events at client companies for whom he had never performed legal work.
- In March 2017, a jury found a former BigLaw patent lawyer guilty of securities fraud. The lawyer purportedly blurted out to his investment advisor that "It would nice to be King for a day," to signal that his client, King Pharmaceuticals Inc., was merging with Pfizer Inc. The lawyer is currently seeking a retrial.
- In September 2016, a federal court sentenced the former managing clerk at a large mergers and acquisitions firm to nearly 4 years for digging up tips in the firm's internal system using search terms like "merger agreement," "bid letter," "engagement letter," and "due diligence." The scheme netted him more than $5.6 million.

22

22

Sources of Lawyers' Data Security Obligations

- Model Rules of Professional Conduct
- State Ethics Opinions
- Fiduciary Duty
- Client Requirements
- Data Security & Data Privacy Laws
- Reputation

23

23

Ensure Technology Competence

Comment 8 to Model Rule 1.1 requires lawyers to know and understand the "benefits and risks associated with relevant technology."

PA Bar Ass'n Formal Op. 2020-300, Ethical Obligations for Lawyers Working Remotely (April 2020) – reminds lawyers to ensure protection of client confidential information

- Zoom, Webex, and other videoconferencing platforms
- VPN, Citrix, home wifi, smart speakers

Train on the use of the firm's document management system and electronic filing systems to manage client files.

24

24

Technological Competence | A Few Examples

- E-Discovery
- Artificial Intelligence
- Cloud Computing
- Encryption
- Technologies used in the courtroom
- Social Media
- Redaction Software
- Spyware
- Videoconference platforms
- Metadata

25

25

The Duty of Confidentiality & Data Security

- The duty of confidentiality imposes an obligation to make "reasonable efforts" to safeguard confidential information against unauthorized access and against inadvertent or unauthorized disclosure.
- Reasonable Efforts? It depends.
  - Sensitivity of information; risk of disclosure without additional safeguards; cost and benefits of additional safeguards; specific client instructions; and data privacy laws, among other factors.

26

26

Protecting Confidentiality – Best Practices

- Encryption and more encryption.
- Use secure networks.
  - Avoid the use of public Wi-Fi with law firm computers or devices carrying confidential client Information.
  - Use a virtual private network (VPN).
- Two-factor authentication.
- Maintain control of devices and thumb drives.
- Secure laptops and smartphones.
- Review and follow the firm's policies on information security.
  - Build a pro-security culture: lead by example.

27

27

Additional Best Practices

- Conduct business calls out of the earshot of other people – and devices.
- Clean desks? Locked doors? Do not leave confidential documents out where others can see them.
- When working on a laptop in a public area, sit with your back to a wall or otherwise position yourself so that no one can read your screen, or use a screen filter.
- Use only firm approved software, including cloud storage, file-share solutions, or flash drives.
  - Refrain from emailing or saving work documents to personal devices, personal email accounts, or portable media.
- Properly dispose of sensitive information.

28

28

See Anything Familiar?

In December 2019, SplashData released its ninth annual "Worst Passwords List," compiled from more than five million passwords leaked during the year. Which of the following passwords DID NOT crack the Top 25 Worst Passwords List?

A. 123456
B. donald
C. iloveyou
D. password
E. qwerty

29

29

The Internet's Worst Passwords and What They May Say About You

- **123456** *I can't be bothered to take even the most basic step to protect my personal information. Seriously, just go ahead and take it.*
- **password** *I failed to understand the question.*
- **password1** *My last password was compromised, so I added a "1" this time for extra security.*
- **111111** *I managed to find one of the few passwords that's both easy to crack and hard to remember. (How many 1s was it, again?)*
- **admin** *I should be fired immediately.*
- **qwerty** *Aren't I clever? My password is written right there on the keyboard.*
- **letmein** Might as well let everyone else in, too.

30

30

Do Not Post Passwords on or Near Device, Part 1

31

31

Do Not Post Passwords on or Near Device, Part 1

32

32

Do Not Post Passwords on or Near Device, Part 2

33

33

Do Not Post Passwords on or Near Device, Part 2

34

34

Password Best Practices

- The National Institute of Standards and Technology (NIST) recommends long passwords that are easy to remember. Overly complex passwords are unnecessary.
  - No dictionary words, names of a person, pet, or sports team
  - Avoid character substitutions like P@$$word for dictionary words, as well as repetitive or sequential characters such as aaaaaaaa or 1234abcd.
  - Do not use a firm password as a personal account password (and vice-versa)
- Georgia Institute of Technology: 8 character password cracked in less than 2 hours; approximately 17,000 years to crack a strong 12 character password.

35

35

More Password Best Practices

- Top Password Managers
  - LastPass, Dashlane, KeePass, 1Password, RoboForm, Password Safe
- Password protect your mobile devices
- Be careful about sharing information online, including on social media. That information can allow fraudsters to guess passwords or answer security questions.

36

36

The Duty to Report Cyber Events

In Novel Case, Insurer Sues Own Law Firm After Data Breach

By Ben Kochman

Law360 (April 13, 2020, 8:55 PM EDT) -- An insurer that offers coverage for cyberattacks has accused a law firm it hired of concealing a data breach, in a Missouri federal lawsuit that industry insiders say thrusts into the spotlight a type of conflict that normally plays out behind the scenes.

37

37

The Ethical Duty to Report a Cyber Intrusion

- Model Rule 1.4 and the general duty to communicate with clients
  - Lawyers must keep clients reasonably informed about the status of matters
  - Lawyers must inform clients about material adverse developments
- Model Rule 1.4 requires client notification if a data breach occurs that results in the unauthorized acquisition of a client's information
  - No ethical duty to report every time a lawyer clicks on a link and malware launched on a computer, or every time a hacker gains access to the law firm's network
  - No ethical duty to report if a client's data is not accessed, acquired, nor compromised during a security incident
  - It may matter if the client's data is encrypted at rest

38

38

Recent Ethics Opinions on Data Security

- California State Bar Formal Opinion 2020-203 (2020):
  Lawyers' Obligations When Unauthorized Third Persons Access Confidential Client Information
- Pennsylvania Bar Association Formal Opinion 2020-300 (2020):
  Ethical Obligations for Lawyers Working Remotely
- ABA Formal Opinion 483 (2018):
  Lawyers' Obligations After an Electronic Data Breach
- ABA Formal Opinion 477R (2017):
  Securing Communication of Protected Client Information

39

39

Law Firms' Top Outside Counsel Guideline Priorities

1. Indemnification
2. Data Security Requirements
3. Client Identity / Corporate Family Relationships
4. Expanded Definition of Conflicts
5. Billing and Fee Requirements
6. Business Competitor / Enterprise Conflicts
7. Conflicts – Generally
8. Advance Waivers / Unwillingness to Provide Prospective Consent
9. Choice of Law
10. "Issues of Interest" Conflicts
11. Most Favored Nation Clauses / Client Billing Rates
12. Diversity Policies
13. IP Rights to Work Product Modify Standard of Care

40

40

Onerous Outside Counsel Guidelines

regulations is required (e.g., Data Privacy/Protection, Export/Import, Patent, Copyright). The firm agrees to defend, indemnify and hold harmless [redacted] from and against any and all allegations, claims, losses and expenses arising out of or relating to a breach, violation or failure to perform or comply with of any of the representations, warranties or obligations set forth herein related to handling [redacted] data. [redacted] agrees that any indemnity provided hereunder shall be strictly excess of any available and collected insurance, from any insurance source, including, but not limited to, the firm's cyber and privacy insurance and its lawyers professional liability insurance. In addition, firm agrees to review all of its liability policies' (including but not limited to its cyber and lawyers professional liability) exclusions and conditions, particularly the liability assumed by contract or similar exclusions (if any), and will seek to have those provisions carved back with respect to this excess indemnification obligation hereunder.

41

41

Strategies to Overcome or Mitigate Onerous OCGs

"Prayer"

"Avoid Insurance Companies"

"None. Ideas Appreciated."

"Pushing back where and when we can. This is too painful to write about."

"Haven't figured that one out yet!"

"Very few ☺"

42

42

General Negotiation Tips | Part 1

- Phone conversations over written communications
- Push back with alternative language
- Demonstrate that suggested revisions better serve client's interests
- Emphasize burden in view of amount of business likely to be received
- Provide copies of firm's internal policies and procedures as a substitute

43

43

General Negotiation Tips | Part 2

- Obtain "side letters" incorporating some of firm's engagement terms
- Accept, but add language clarifying how the firm interprets a provision
- Discuss specific conditions at the firm, or specific aspects of the firm's business model, which make a specific provision difficult or impossible
- Prepare a list of commonly confronted items and standard responses
- Route problematic provisions to designated firm experts or negotiators

44

44

Specific Negotiation Tips

Conflicts

- Request list of business competitors and client corporate affiliates
- Push back on issue conflicts when the firm only represents the client in certain fields and it has no idea what the client's position on other issues may be

Data Security

- Adopt clearly defined data security policies and procedures
- Hire outside consultants to certify firm's security systems, or conduct penetration and vulnerability testing and provide written reports on results
- Use a dedicated information security team to make clients comfortable

Indemnification

- Discuss risk of jeopardizing insurance coverage
- Narrow overly broad causation terms and delete "hold harmless" language

Data Security and Data Privacy Laws

- California Consumer Protection Act (CCPA)
- General Data Protection Regulation (GDPR)
- New York SHIELD Act
- HIPAA & HITECH (personal health information)
- Federal Trade Commission Act (unfair trade practices)
- State Data Breach Notification Laws
- State Document Destruction Laws
- Gramm-Leach-Bliley Act (personal financial information)
- Fair Credit Reporting Act (credit reports)

Final Thoughts

For more information, please contact:

Douglas R. Richmond
Managing Director
+1.312.339.2003
douglas.richmond@aon.com

Henry S. Bryans
Senior Consultant
+1.610.995.0488
henry.bryans@aon.com

Matthew K. Corbin
Senior Vice President and Executive Director
+1.816.225.5815
matthew.corbin@aon.com

Jennifer Finnegan
Senior Vice President and Executive Director
+1.609.203.4903
jenny.finnegan@aon.com

Jane Hunter
Executive Director and Senior Vice President
+44 (0)20.7086.2160
jane.hunter@aon.co.uk

Mark J. Peterson
Managing Director
+1.402.203.5396
mark.peterson1@aon.com

Mark A. Webster
Vice President and Director
+1.913.201.3446
mark.webster1@aon.com

aon.com/professional-services