Douglas Chandler & David Moon- *Cyber Risks & Legal Malpractice*

Douglas Chandler- Co-Founder and Executive Committee Member of the State Bar of Georgia Professional Liability Section, and an active lecturer and panelist on the topics of Law Firm Risk Management, Legal Professional Ethics, and Malpractice Prevention. He has been recognized multiple times by his peers and Atlanta Magazine as a Super Lawyer and Legal Elite by Georgia Trend Magazine.

David Moon graduated from Georgia Tech with an Master of Science – Electrical Engineer in 1993. While attending GA Tech, he was a founding father of the GA Tech Delta Chi fraternity which rapidly grew top chapter in the National Fraternity Organization. Upon completion of his degree, David started Lan-Tech, Inc., a company speculating in legal technology for law firms. The business grew to include some of the prominent law firms in Atlanta. He is also a partner is CompassPOINT Legal, LLC. David Moon has received a number of certifications and awards through out the years. He is currently an STI Tabs3 President Circle Member. In 2005, he was the recipient of the Legal Technology Consultant of the Year (a life time achievement award). He has certifications in Summation, Concordance, Time Matters, Billing Maters, Citrix, Tabs3 and Practice Master. Over the years, David has consulted with attorneys as an expert witness in computer technology and legal software. David Moon has transitioned Lan-Tech, Inc. into a legal cloud hosting desktop and servers. He designed the infrastructure and security to give law firms the ability to work from any location and use the traditional apps they have always relied upon.

1 **Risk Management, Cyber Security, and Professional Liability**

American Board of Professional Liability Attorneys: National Legal & Medical Malpractice Conference
May 6, 2017

2 **Introductions**

Douglas Chandler
Co-Founder, Chandler & Moore Law LLC, Atlanta, GA
ABPLA Diplomate
douglas@chandlermoorelaw.com

David Moon
Principal/Partner Lan-Tech, Inc. / Compass Point Legal, LLC, Atlanta, GA
20+ years in legal technology and information security
david@lan-tech.com

3 **Cybersecurity or Cyberrisk**
Biggest Law Firm Risk in 2017

- TruShield, an IT security company, reported in 2015 that the legal industry was the second most targeted sector for a cyber attack.
- The TruShield 2016 report revealed that small law firms were now the most targeted.
- Cravath/Weil-On March 29,2016, the Wall Street Journal reported that hackers had broken into the files of some of the biggest law firms in an insider-trading scheme that involved planned mergers. The press release linked the hacks to three foreign nationals who used information stolen from the firms for insider trading, gaining more than $4 million.

4 **Cybersecurity or Cyberrisk**

Biggest Law Firm Risk in 2017, Cont.

- Oleras—In February 2016, an alert went out to 46 law firms in the United States and two law firms in the U. K. that Ukraine-based hacker Oleras was advertising phishing services on a Russian website. According to the Wall Street Journal, this was related to the March 2016 breaches of several major law firms.

5 **Lawyer Duties and Obligations Come From Where?**

- Clients pass their own obligations to their lawyers:
  - Consumer Financial Protection Bureau (CFPB)
  - New York State Department of Financial Services (NYDFS) recently promulgated cyber regulations for financial institutions that are likely to increase the risks to directors & officers (D&Os), resulting in an increase in claims.

6 **Cyber Breach = Malpractice? Really?**

- On April 18, 2016, a New York couple filed a complaint against their real estate attorney based on their falling victim to a social engineering data breach.
- The couple's two-count complaint alleged claims for legal malpractice and breach of fiduciary based on their attorney's use of an AOL email account that allegedly contributed to cyber-criminals being able to hack into the attorney's account and perpetrate an elaborate wire-transferring heist of almost $2 million in the client's funds. Robert Millard, et al v. Patricia L. Doran.
- https://www.scribd.com/document/309730357/NYC-Complaint

7 **Law Firm Protection**
Planning, Investment, Training

- Can no longer relegated to IT or General Policy
- Part of Doing Business Everyday
- Roadblock to Proper Preparation-- $$$$

- Minimum Requirement—Up to Date Software
- When problems occur must have a specific plan

8 **Lawyer and Non-lawyer Training**

Employees-- your weakest link?

- Train annually and upon hire
- Train on cybersecurity protocol
- Train on spotting issues
- Train on reacting to issues
- Create anonymous hotline or suggestion box
- Encourage open discussion – experiences, feedback, and ideas
- Written policies and protocol – signature of acceptance
- Reinforce THE USER is responsible

9 **The A.R.T. of Risk Management**

- Avoid
  - Don't undertake responsibility outside of your competency
  - Specifically define parameters for firm members
    - *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms and Business Professionals* will be published before the ABA Annual Meeting in August.
    - *Cybersecurity for the Home and Office: The Lawyer's Guide to Take Charge of Your Own Information Security,* by John Bandler, Available July 2017, ABA Website
    - https://cybersecuirtyhomeandoffice.com/book and https://www.bandlerlaw.com/articles.html
- Retain
  - Self-insure to a minimum with assessments, planning, and training
  - Invest in up-to-date assets
- Transfer
  - Outsource to vendors

- Purchase appropriate cyber coverage

10 **Don't Violate Rule 1.1 Competency- A.R.Transfer**

David Moon

Principal/Partner Lan-Tech, Inc. / Compass Point Legal, LLC
20+ years in legal technology and information security
david@lan-tech.com Founding Partner

- David graduated from Georgia Tech with an Master of Science –Electrical Engineer in 1993.
- David started Lan-Tech, Inc., a company specializing in legal technology for law firms.
- Certifications in Summation, Concordance, Time Matters, Billing Matters, Citrix, Tabs3 and Practice Master.
- Awards include an STI Tabs3 President Circle Member. In 2005 he was named the Legal Technology Consultant of the Year (a life time achievement award).
- David consults as an expert witness on computer technology and legal software topics.

11 **Law Firms Under Attack**

Security Experts say Hackers are targeting law firms.

- 80 of the 100 biggest firms in the country have been hacked
- McKenna Long & Aldridge (now Dentons) lost Social Security numbers
- Looking for potential corporate mergers, patent, trade secrets, litigation plans, personal information

12 **Law Firms Under Attack**

- Law360 (Sept 22, 2015) – ABA survey has found 1 in 4 law firms with at least 100 attorney have experience a breach

13 **Law Firms Under Attack**

"Series of security breaches that struck prestigious law firms last year was more pervasive than reported . . ."

"The incident involved hackers getting into the email accounts of partners . . ."
Dec 7, 2016 – Fortune

14 **Law Firms Under Attack**

Many believe they are too small to warrant attack
Why would hackers go after us little guys?

- Easy targets
- Valuable information
- Ability to pay
- Not likely to report

15 **Easy Targets**

Citigroup, for example, recently told its employees in an internal report that law firms are vulnerable hacking targets because they are clearinghouses of high-value information and possess relatively weak security measures, according to The New York Times. The Citi memo also said that law firm security generally falls below the standards of other industries — and pointed to a reluctance by law firms to publicly disclose breaches and the absence of formal reporting requirements in the legal field as reasons for silence.
http://www.nytimes.com/2015/03/27/business/dealbook/citigroup-report-chides-law-firms-for-silence-on-hackings.html?_r=1

16 **Security Attack – A matter of when**

All systems are vulnerable – all systems will have some breach at some point!

In 2003, former FBI director Robert Mueller stated "There are only two types of companies: Those that have been hacked, and those that will be."

What is your annual Security Budget?

- Don't have one?

- Should be a separate line item beyond IT budget

17 **Security Attack – A matter of when**

The goal is to:

- Minimize the risk
- Minimize the damage
- To know what was accessed.
  - Some software can audit all data access, by user and when. Great tool for knowing what was breached and the extent of damage.

18 **Client Security Assessment**

- 2016- 30.7% of all law firms and 62.8% of firms over 500 lawyers report clients provide security requirements
- Corporate clients are requiring law firms to complete security assessments
  - Email Encryption
  - Storage of data
  - Written policy to handle breach
  - Employee policy/training

19 **Morgan Stanley Sample Questionnaire**

20 **Morgan Stanley Sample Questionnaire**

21 **Law Firms Under Attack**

Cyberinsurance

- Market is relatively small and new

Are there any requirements?

- Security audits
- Reasonable care

22 **Hacking is a big business**

Why are they attacking law firms?

- Corporate Espionage
- Selling/using personal information
- Ransom
- Blackmail

23 **Ransomware**

CryptoLocker / Cryptowall

- What is it?
- How do you get it?
- Trying to prevent it
- New Variations
  - Fear is one day it will run for days before announcing itself
- Pay the ransom or Restore – Only options

24 **Hackers Go Fishing**

25 **Example of spoof email**

26 **Example of spoof email**

27 **Example of spoof email**

28 **Silently Steal Data**

Dear Law Firm,

We have a copy of all your client's data. To prove we have a copy, here is some of the files we have.

Unless you pay us this amount of money, we will publish ALL of the firms data which includes your clients confidential data, to public servers for the world to see.

29 **Rules of Professional Conduct**

Rule 1.6, Confidentiality of Information, states that lawyers shall not disclose private information and shall make *reasonable*

efforts to prevent any such disclosures.

What are *Reasonable Efforts*?

30 **Unique Professional Responsibility**

What if you had a breach of a client's files, and that breach involved personal information of the client's customers?

Codes of ethics generally dictate that attorneys must not reveal information related to the representation of clients, and must make reasonable efforts to prevent unauthorized access to client secrets. Firms that suffer security breaches face questions about what steps they took to meet the latter obligation, while the act of disclosing the breach itself challenges the confidentiality demanded of the former.

31 **State Laws on Disclosure of Data Breach**

- Forty-eight states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information.
- http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

32 **Road To Protection**

Education

- Attorneys and Staff
  - Written standards
  - No one should be above requirements or exempt
  - Educating new hires
- Client
  - Communication with clients
  - Email Encryption

33 **Social Engineering Hacking**

- People are the weakest link
- Easily tricked into giving up information or opening the door
  - Running a backdoor
  - Security questions for forgot passwords
- Trust No One!

34 **Passwords**

The obvious is still overlooked

- Min 8 Characters – Randomize
  - P@ssw0rd is no longer acceptable
- Use different passwords from other systems such as Social Media, Banking, Etc

35 **Fishing/Spoofing Emails**

- Cannot stop someone from sending out emails pretending to be from you or appearing to come from someone you know
  - Email sender address easily faked
  - Be suspicious of attachments (Not expecting, never open)
  - Even encrypted email can be faked (has link to log in)
- Test peoples awareness and following the rules

36 **Not work related – stay off**

- Social Media attacks – i.e. Facebook
  - Breach is typically from all the links to other pages
  - Friend Request should be under scrutiny

37 **Protection vs Publicity**

- Firm Web – What information are you giving out
  - Hackers targeting your client with search the web and target the firm.
  - Yes, information could be gathered from Court documents
  - Attorney Email address – Also obtained from Ga Bar web site
    - Spoofing an attorney email address allows for each breach.

38 **Email Breach**

Breach is difficult to detect

- So many devices connect and ways to connect
  - Outlook on PC
  - Web Access
  - Smart Phone
  - Tablet

39 **Email is not a long term storage**

One breach email account can compromise TENS of THOUSANDS of emails going back many years

Any confidential documents should not be attached to email – but we all do it.

40 **Smart Phones**

- Password protect your phone
- Setup a remote wipe feature if your phone is lost or stolen
- Change your email password
- New security attacks are possible through unopen text messages (Stagefright)
- Do not install apps that are not needed
  - Only install apps from the App Store
  - Ad producing apps make it possible for other apps not going through the apps store
- Setup firm policy for users the use a personal phone to access email and other firm resources.

41 **Laptops and USB Drives**

- All easily stolen storage needs to be encrypted.
- Laptops can have tracking software installed with remote wipe features.
- Avoid coping data to Laptops and USB drives.

42 **Secure Your Offices**

High rise office buildings are as vulnerable as the private office

space – maybe more vulnerable

- Secure your Severs
  - Locked server room
  - Cameras
- Log off your computers when leaving
- Lobby / reception area should be secured from the rest of the office

43 **Secure Your Office**

- Placement of computers and monitors
  - Monitor should not be visible from any guest sitting area or window
  - Keyboard should not be visible when others are present (typing a password)
  - Computer should not be accessible by others (computer on the side of desk / front or back – Keyboard loggers can be connected easily.
- No one should be left alone where there is a computer or even a network connection.
- WiFi with strong encryption. Guest WiFi should be isolated from network.

44 **Home Access to Office Computer and Data**

- Home computers may be the biggest weak link.
- Remote Node connections (VPN) which the home computer has a direct connection to server drive can unleash ransomware or cause data breach.
- Remote Control connections will isolate remote (home) computer better – Citrix/Terminal Sever, LogMeIn, GoToMyPC.
- Home computers could have keyboard loggers which grab user names and passwords.

45 **Cloud Computing – Secure or Not**

- Many myths about Cloud Computer Security
- Know the cloud vendor

- One who specializes in legal
- Much (Not All) of the security is shifted to the Cloud vendor. But, is liability shifted?

46 **New Ransomware Attack**

- Using RDP and weak passwords
  - Some compromised TeamViewer accounts (IT providers) have been used to spread attacks

47 **Cloud Computing**

- Some Cloud Services could actually introduce vulnerabilities.
  - Can Dropbox create a security hole?

48 **State Bar - Cloud**

- ABA list state bars who have issued opinions
- http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html

49 **Cloud Computing Ethics Opinions**

- ALABAMA
  Opinion 2010-02
- Use Permitted: Yes
- Standard: Reasonable Care
- Requirements and Recommendations:
  - Know how provider handles storage/security of data.
  - Reasonably ensure confidentiality agreement is followed.
  - Stay abreast of best practices regarding data safeguards.
- https://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html

50 **Security is never finished**

- Securing your firm's and your clients' information is an

ongoing initiative, the strength of which lies with each individual user.

- Consult, Design, Implement, Train, Repeat

51 **When Problems Occur - Respond**

Don't panic, but also don't stick your head in the sand!

- Consult the firm's plan
- Appropriate, timely response to carrier and client is critical
- Communication is critical, but not necessarily from you
  - Seek competent advice
  - Read your policy

52 **Contact Information**

Douglas V. Chandler, Chandler & Moore Law, LLC
douglas@chandlermoorelaw.com
770-751-8050
www.chandlermoorelaw.com
LinkedIn Group: bit.ly/attorneyethicsgroup

David Moon, Lan-Tech, Inc. / CompassPOINT Legal, LLC
david@lan-tech.com
770-514-0400 x212
www.compasspointlegal.com

53 **Thank You!**