

# **Data Breach Risks for Law Firms\***

Presented by

**Elizabeth Rogers**

**David Coker**

Presented to

**With Technology and  
Justice for All**

for the State Bar of Texas  
Computer and Technology Law  
Section

**December 1, 2017**

\* Original content prepared by Elizabeth  
Rogers and Pierre Grosdidier

# Statistics and Types of Breaches

- 34% of 100 law firms have had clients request a security audit
  - Large clients are now routinely sending security due diligence questionnaires (Large banks, Hospitals, etc)
- Most common types of breaches:
  - Loss or theft of laptops, thumb drives, smart phones or tablets
  - Phishing
    - December 2, 2016 – NYAG warned law firms not to click on a link claiming to reveal a complaint lodged by a client
  - Employees/third parties using unauthorized hardware and software (Evernote/Google Drive)

# Law firms are great targets for cybercriminals

- Environment
- While the biggest law firms have put a series of top-level security measures in place, the vulnerability lies in compliance among all attorneys at a firm
- Some attorneys and staff may not fully grasp the insecurity of behavior such as:
  - using public networks to access client documents
  - Unencrypted email transmission

# Most common types of hackers

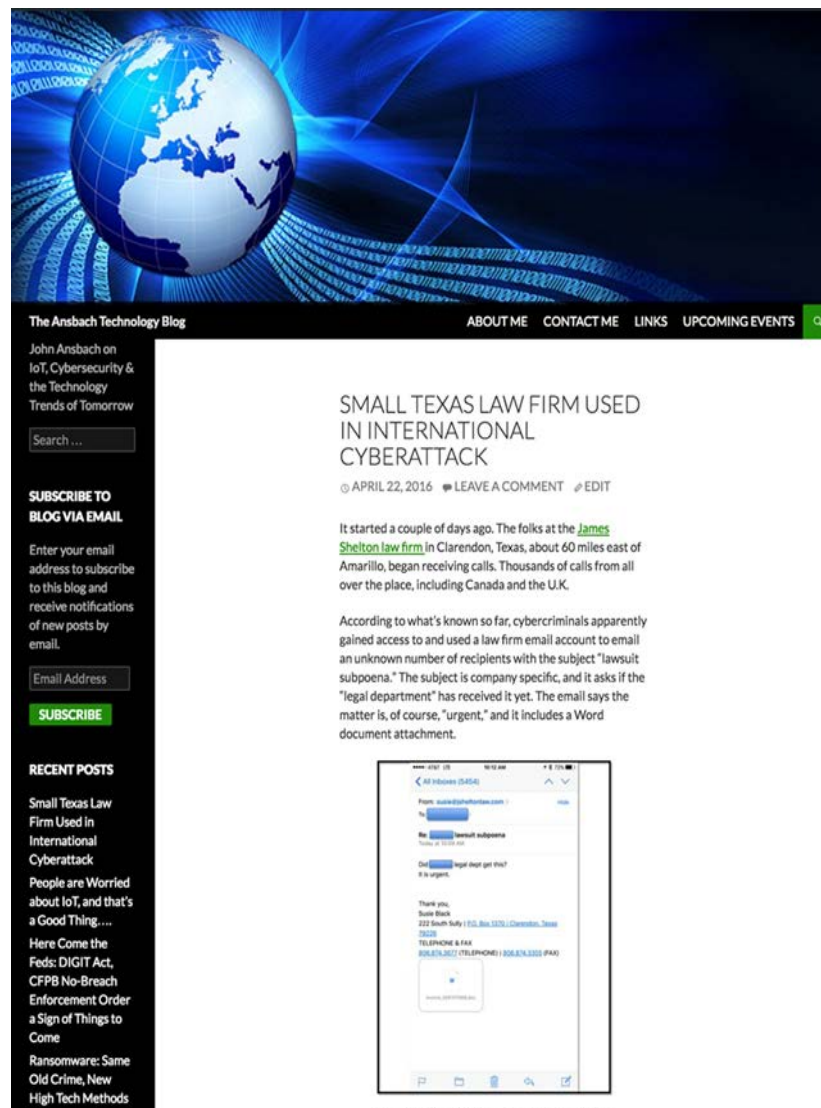
- \*\*Cybercriminals
  - Theft is motive
- #1 law firm hacker
- Hacktivists
- Nation state hackers
- Insider Threats
  - Malicious
  - Negligent



# Even in Clarendon, Texas....

## Small Texas Law Firm Used in International Cyberattack

Cybercriminals apparently gained access to and used a valid law firm email account to email an unknown number of recipients with the subject 'lawsuit subpoena.' The email contained malware that attackers could use to steal banking credentials and other personal information..."



The Ansbach Technology Blog

ABOUT ME CONTACT ME LINKS UPCOMING EVENTS

John Ansbach on IoT, Cybersecurity & the Technology Trends of Tomorrow

Search ...

SUBSCRIBE TO BLOG VIA EMAIL

Enter your email address to subscribe to this blog and receive notifications of new posts by email.

Email Address

SUBSCRIBE

RECENT POSTS

Small Texas Law Firm Used in International Cyberattack

People are Worried about IoT, and that's a Good Thing....

Here Come the Feds: DIGIT Act, CFPB No-Breach Enforcement Order a Sign of Things to Come


Ransomware: Same Old Crime, New High Tech Methods

### SMALL TEXAS LAW FIRM USED IN INTERNATIONAL CYBERATTACK

© APRIL 22, 2016 LEAVE A COMMENT EDIT

It started a couple of days ago. The folks at the [James Shelton law firm](#) in Clarendon, Texas, about 60 miles east of Amarillo, began receiving calls. Thousands of calls from all over the place, including Canada and the U.K.

According to what's known so far, cybercriminals apparently gained access to and used a law firm email account to email an unknown number of recipients with the subject "lawsuit subpoena." The subject is company specific, and it asks if the "legal department" has received it yet. The email says the matter is, of course, "urgent," and it includes a Word document attachment.



# Brief Overview of Law Firm Hacking History

- MARCH 2016
- Major law firms Cravath Swaine & Moore and Weil, Gotshal and Manges are hacked
- it is suspected that the attackers were targeting information that could be used for insider trading scheme.



# Brief Overview of Law Firm Hacking History

- APRIL 2016
- Panamanian law firm, Mossack Fonseca, is hacked resulting in a data breach of 11.5 million records totaling over 2.6 terabytes of data in total. The leaked information exposed a network of shell companies used in tax evasion schemes.
- That's enough to fill 81 USB drives of 32 GB worth of data.
- The firm's customer facing WordPress website was running an outdated/vulnerable version of a plugin called 'Revolution Slider' that enabled a hacker to exploit a well known bug and gain access to its mail servers hosted on the same IP network

**December 27, 2016**

## **Indictments Against 3 Chinese Traders Unsealed in Manhattan Related to Law Firm Hack**

- 2 Prominent International Law Firms with Offices in NYC
- Law Firm #1
- Compromised employee credentials allowed Web Server Access and from Web Server, traders got access to Email Server
- Read privileged and confidential emails of partners working on 2 separate acquisitions, including offer price for target corporations.
- Defendants caused approximately 2.8 gigabytes of confidential data to be exfiltrated from the Law Firm-1 Email Server during negotiations involving Intel's acquisition of Altera between April 2014 – late 2015.
- Sold shares at \$1.4 million profit



**December 27, 2016**

## **Indictments Against 3 Chinese Traders Unsealed in Manhattan Related to Law Firm Hack**



- Law firm #2 hacked in April and May of 2015
- Exfiltration of confidential/privileged information related to Pitney Bowes Acquisition of Borderfree ecommerce site.
- Traders profited by \$814,000 during sale of stock
- Five other law firms were unsuccessfully targeted on more than 100,000 occasions between March and September 2015.

# Technological competence = Ethical duty of professional responsibility?

- ABA Annual Meeting in August of 2012
- Addition of language to the Comment to Model Rule 1.1 (Duty of Competence)
  - [8] 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 technology...
- 28 states have adopted Model Rule. 1.1 (Not Texas)
- The amendments also added the following new subsection (highlighted) to Model Rule 1.6 Confidentiality of Information
  - (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.

# ABA Model Rule Amendments for Ethical Duty of Technological Competence

- ABA Model Rule 1.6 Duty to Protect Client Data covers two behaviors – inadvertent disclosure and unauthorized access
  - Inadvertent disclosure includes
    - threats like leaving a briefcase, laptop, or smartphone in a taxi or restaurant
    - Sending a confidential e-mail to the wrong recipient
    - erroneously producing privileged documents or data, or
    - exposing confidential metadata.
- Unauthorized access includes threats like
  - hackers, criminals, malware, and
  - insider threats

# ABA Model Rule Amendments for Ethical Duty of Technological Competence

>Noteworthy are these changes to Comment [18] of Rule 1.6-Acting Competently to Preserve Confidentiality

- [18] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client
  - against unauthorized access by third parties, and
  - against inadvertent or unauthorized disclosure by the lawyer or other persons or entities who are participating in the representation of the client or who are subject to the lawyer's supervision or monitoring.

# ABA Model Rule Amendments for Ethical Duty of Technological Competence

- The unauthorized access to, or the inadvertent or unauthorized disclosure of confidential information does not constitute a violation of paragraph(c) if the lawyer has made reasonable efforts to prevent the access or disclosure.
- Factors to be considered in determining the reasonableness of the lawyer's efforts include:
  - the sensitivity of the information,
  - the likelihood of disclosure if additional safeguards are not employed
  - 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).

# Texas Ethics Opinion 648

## April 2015

- QUESTION PRESENTED
  - Under the Texas Disciplinary Rules of Professional Conduct, may a lawyer communicate confidential information by email?
- FACTS
  - Most of a law firm's written communication is delivered by web-based email, such as unencrypted Gmail.



# Texas Ethics Opinion 648

## April 2015

- DISCUSSION
  - Rule 1.05(b) provides that, except as permitted by paragraphs (c) and (d) of the Rule:
    - “a lawyer shall not knowingly:
      - (1) Reveal confidential information of a client or former client to:
        - » (i) a person that the client has instructed is not to receive the information; or
        - » (ii) anyone else, other than the client, the client’s representatives, or the members, associates, or employees of the lawyer’s law firm.

# Texas Ethics Opinion 648

## April 2015

- **CONCLUSION:** Email communication is proper. Considering the present state of technology and email usage, a lawyer may generally communicate confidential information by email.
- Some circumstances, may, however, cause a lawyer to have a duty to advise a client regarding risks incident to the sending or receiving of emails arising from those circumstances and to consider whether it is prudent to use encrypted email or another form of communication.
- The risk an unauthorized person will gain access to confidential information is inherent in the delivery of any written communication including delivery by the U.S. Postal Service, a private mail service, a courier, or facsimile.
- Persons who use email have a reasonable expectation of privacy based, in part, upon statutes that make it a crime to intercept emails. (ECPA)



# ***Shore v. Johnson & Bell***

- Class action suit
- “Johnson & Bell [wa]s a data breach waiting to happen.”
- No actual harm
- Showcase article
- Moved to arbitration



# The FTC and data security

- Main federal agency re. data security
- Authority in FTC Act
  - 15 U.S.C. 45 ("Section 5")
- Close to 60 FTC settlements since 2002
- Key case
  - *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015)
    - Three breaches in 2008–10
    - 600,000 credit card; \$10.6m in fraud
    - Holding: Section 5 authorizes FTC to regulate cybersecurity

# ***FTC v. Wyndham Worldwide Corp.***

- It is inequitable to:
  - promise security to attract customers;
  - fail to deliver with poor security;
  - “expose unsuspecting customers” to harm;
  - and keep the profits.

# FTC Act Sections 5(a), (n)

- “[U]nfair or deceptive acts or practices in or affecting commerce, are . . . unlawful.”
- Unlawful as unfair if “the act or practice
  - causes or is likely to cause substantial injury to consumers
  - which is not reasonably avoidable by consumers themselves and
  - not outweighed by countervailing benefits to consumers or to competition.”

# *In re LabMD, Inc., FTC No. 9357*

- 



---

**TIVERSA, INC.: WHITE KNIGHT OR HI-TECH PROTECTION RACKET?**

---

# ***In re LabMD, Inc. Complaint***

- Complicated procedural history
- Initial Decision: ALJ dismissed the FTC complaint (Nov. 13, 2015)
- Full Commission reverses (July 29, 2016)
- Next steps
  - Reconsideration
  - Appeal to Circuit Court

## ***LabMD: the FTC's arguments***

- A company's lax computer security measures create a significant risk of concrete harm and are likely to cause substantial consumer injury.
- *Proof of actual identity theft is not required.*
- Under this argument, Section 5 liability can be imposed merely based on the risk that inadequate security measures will cause a data breach that will cause future harm.

## ***LabMD: The ALJ's arguments***

- FTC had “proven the ‘possibility’ of harm, but not any ‘probability’ or likelihood of harm.”
- Finding that consumers likely to suffer future harm “would require speculation upon speculation.”
- FTC should concern itself with “substantial” injuries, and not “trivial or merely speculative harm.”



# ***LabMD: Commission's arguments***

- Release of 1718 File breached Section 5
- 11-month 1718 File exposure is a breach
  - Created “significant risk” of substantial consumer injury
- Commission punts on whether inadequate security alone constitutes a breach
  - “[W]e need not address Complaint Counsel’s broader argument.”

# *LabMD* eight years after the breach

**Feds raid 'extortionist' IT security biz Tiversa,  
CEO put on leave**

And whistleblower defamation suit dropped



Anonymous Twitter user Laserwolf snaps a pic of the Feds as they line up to raid Tiversa



# *LabMD* eight years after the breach



# What's one to do?

- Commission Statement of Jan. 31, 2014
- FTC “does not require perfect security”
- Requires “reasonable and appropriate security” through “***a continuous process***”
- “[N]o one-size-fits-all data security program”
- “[M]ere fact that a breach occurred does not mean” a violation of the law
- FTC-published guidelines

# FTC publications re. data security

- Protecting Personal Information, 2011
- Start with Security; lessons learned from FTC cases, 2015
- Cases that did not follow the guidelines:
  - *In re LabMD, Inc.*, FTC No. 9357
  - *In re Adobe Systems Inc. Privacy Litigation*, No. 13-cv-05226-LHK, 2014 WL 4379916 (N.D. Cal. Sept. 4, 2014)
  - *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015)

# Things LabMD did wrong

- No data purge (100,000 unneeded records)
- No access segregation
- No password policies ("labmd")
- No unauthorized access detection
- No effective antivirus and firewalls
- No risk assessments
- No security training
- No security program
- Haphazard, reactive, ineffective inspections



# Things Adobe did wrong

- Hackers stole and decrypted credit card nos.; code
- Quotes from the opinion:
  - “Adobe’s security practices were deeply flawed”
  - “did not conform to industry standards”
  - “encryption scheme was poorly implemented”
  - “Adobe . . . failed to
    - employ intrusion detection systems,
    - properly segment its network, or
    - implement user or network level system controls.”

# Things Wyndham did wrong

- Three attacks in three years
- Default user ID and password (“micros”) – Micros Systems, Inc.
- No firewalls
- Out-of-date operating system
  - No security update in over three years
- No third-party access restrictions
- No unauthorized access detection
- No security investigations



# Recent FTC settlement



FEDERAL TRADE COMMISSION  
PROTECTING AMERICA'S CONSUMERS

Contact | Stay Connected

Search

- LifeLock breached a federal court order
- LifeLock
  - Failed to deploy a security program
  - Falsely advertised safeguards
  - Falsely advertised breach notices
  - Failed to maintain records
- ***\$100 million***

# Do not rest on your laurels



FTC Statement: "security is a continuous process of assessing and addressing risk."



**Audit your system security  
Get second opinion**

# Have a data breach plan

- Security is now a Legal-IT joint effort



# Data breach consequences & issues

- Huge, costly distraction
  - Forensic and legal investigations
  - Crisis management
- Class actions
  - Consumers
    - Target breach: 10¢ per consumer
  - Vendors
  - Shareholders
  - Banks
    - \$8 per card replacement cost
- Data breach insurance policy terms?

# Q & A

