Every Firm is a Target:

Lawyers' Ethical Duties Regarding CyberSecurity

Presented by:
Larry H. Kunin
Morris, Manning & Martin, LLP

The Florida Bar
June 13, 2018

MORRIS, MANNING & MARTIN, LLP

Today's Presenter

Larry H. Kunin

Partner, Commercial and Technology Litigation
Partner & Chair, Data Protection & Breach Practice
Morris, Manning & Martin, LLP
Direct: 404.504.7798
lkunin@mmmlaw.com

Data Breaches Are Increasing

"Not if, but when… and how."

- *Average* cost is $4 million per breach.
- Average cost per stolen record is $158.
- Guidance follows this position.
- Expect to see additional requirements for compliance efforts.

What is a Data Breach?

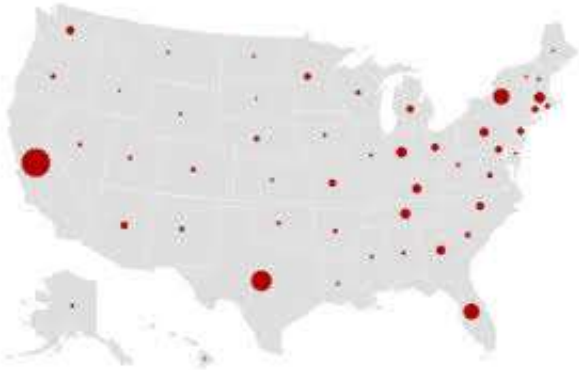
- Online hacking
- Intercepting data transmissions
- Lost/stolen equipment
- Accidental disclosure
  - Wrong autocomplete
- Storage media, etc.
- Disposed equipment
- Unsecure papers

Who is Being Impacted

- White Lodging: Twice hacked through ancillary hotel services
- Wyndham: Hacked multiple times. Sued by FTC under allegation that Wyndham's privacy policy misrepresented security measures
- Target: Credit card breach
- Sony: Embarrassing emails disclosed
- Orient Express: Access to corporate email exposed credit card data

Data Types and Related Liability

- Electronic personally identifiable information is subject to:
  - A patchwork of federal and state legislation
  - Layers of liability based on the type of data
    - Payment card information
    - Consumer personally identifiable information
    - Individual health information (HIPAA)
    - Other non-public personal information



- State notification requirements (47 states) are based on residency of victim.
- PCI focuses on credit cards – other payment transactions, such as ACH & debit, have additional regulatory overlay.

Why Should Lawyers Care?

- A law firm a business that possesses financial data, payment data, patient health data ("PHI"). Law firms may thus be subject to:
  - Payment Card Industry ("PCI") standards
  - HIPAA
  - Contractual security obligations
- Estimated the 80% of the largest 100 law firms have experienced *(Peter Tyrell, CEO of Digital Guardian*)

Why Should Lawyers Care?

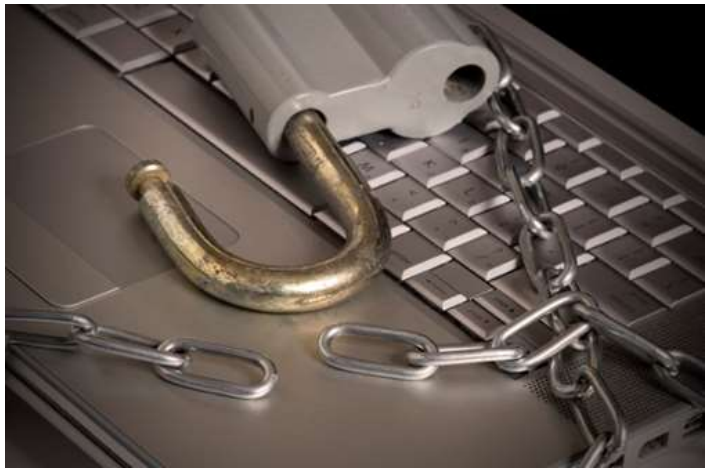
- ATTORNEY-CLIENT PRIVILEGE
- Hacker could access privileged emails and documents
- Emails and documents could also contain insider information
- This concern affects ***outside and in-house counsel***

Where Does Client Data Reside?

- Email Server
- Document Database
- Workstations
- Smart phones and tablets
- Flash drives
- Home PC
- Cloud
- Paper
- Vendors (printers, eDiscovery, experts, storage)
- Personal email?

Common Risk Points

- Shared or weak passwords
- Insecure computer servers
- Information residing on unprotected mobile devices
- Insecure wi-fi access points
- Untrained employees
- Insecure disposal
- Use of insecure home PC
- Losing papers, flash drives
- Wandering Eyes (especially on airplanes)



Phishing "Dear Counsel" Scams

- "Please advise if your firm handles breach of contract case."
- "Are you a firm that handles purchase and sale transactions."
- Some are very good at spoofing real names and addresses.
- If you hit "reply" (do not actually send) is the response email address the same?
  - Example, email from Gareth Drenth replies to lnguyen.3h@gmail.com
  - Email from "Oaki" replies to hazel88@primus.com.au
- Assume all are scams, and proceed VERY carefully

Florida Ethical Rule 4-1.1

Competence

A lawyer shall provide competent representation to a client. . . . Competence requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Florida Ethical Rule 4-1.6

Confidentiality Of Information

a. Consent Required to Reveal Information. A lawyer must not reveal information relating to representation of a client except as stated in subdivisions (b), (c), and (d), unless the client gives informed consent..

* * *

e. Limitation on Amount of Disclosure. When disclosure is mandated or permitted, the lawyer must disclose no more information than is required to meet the requirements or accomplish the purposes of this rule.

Florida Ethical Rule 4-5.3

Responsibilities regarding nonlawyer assistants

(b) With respect to a nonlawyer employed or retained by or associated with a lawyer:

1. a partner, and a lawyer who individually or together with other lawyers possesses managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;

2. a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer;

Florida Ethics Opinion 10-2

A lawyer who chooses to use Devices that contain Storage Media such as printers, copiers, scanners, and facsimile machines must take reasonable steps to ensure that client confidentiality is maintained and that the Device is sanitized before disposition, including:

(1) identification of the potential threat to confidentiality along with the development and implementation of policies to address the potential threat to confidentiality;

(2) inventory of the Devices that contain Hard Drives or other Storage Media;

(3) supervision of nonlawyers to obtain adequate assurances that confidentiality will be maintained; and

(4) responsibility for sanitization of the Device by requiring meaningful assurances from the vendor at the intake of the Device and confirmation or certification of the sanitization at the disposition of the Device.

Florida Ethics Opinion 12-3

Lawyers may use cloud computing if they take reasonable precautions to ensure that confidentiality of client information is maintained, that the service provider maintains adequate security, and that the lawyer has adequate access to the information stored remotely. The lawyer should research the service provider to be used.

ABA Ethics Opinion 477

- Updates Ethics Opinion 99-413 (confidentiality in email), which was issued before common use of BYOD and cloud storage.
- “Each device and each storage location offer an opportunity for the inadvertent or unauthorized disclosure of information relating to the representation, and thus implicate a lawyer’s ethical duties.”
- Cites Model Rule 1.1, Comment 8, which states that lawyers must be aware of “the benefits and risks of associated with relevant technology.”
- The opinion addresses the duty to ensure confidentiality via “reasonable efforts.”

New York Ethics Opinion 842

Recommends the following due diligence for cloud computing:

1. Ensuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information;

2. Investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances;

3. Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored.

Other Ethics Opinions Related to Cloud Computing

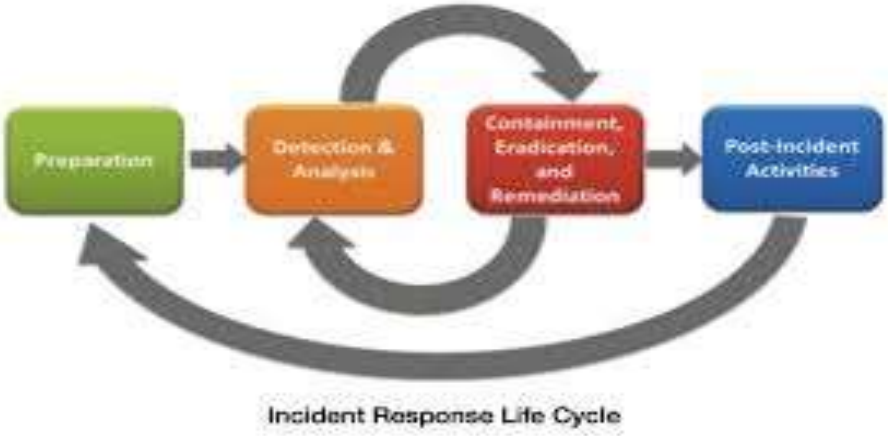
- Alabama Ethics Opinion 2010-02 (reasonable steps to ensure data is protected);
- Arizona Ethics Opinion 09-04 (reasonable precautions to protect confidentiality);
- Iowa Ethics Opinion 11-01 (due diligence steps include ensuring adequate access to the stored information, restrictions, encryption, password protection, what happens to data upon default or termination)
- Nevada Ethics Opinion 33 (third party agreement to confidentiality);
- New York State Bar Ethics Opinion 842 (2010) (stay informed of technological advances and changes in law that could affect privilege);
- Pennsylvania Ethics Opinion 2011-200 (must ensure (1) materials remain confidential, and (2) reasonable safeguards to prevent breach and data loss)

Other Sources of Security Duties

- Common Law: Restatement (3rd) of the Law Governing Lawyers, Sections 16(2) (competence) and 16(3) (confidentiality).
- Contract duties, especially for clients in regulated industries such as financial services and health care.
    - *PCI is a contract duty*
- HIPAA
- HITECH
- 47 State Breach Laws

Security Incident Response Plan (IRP)

- Call lawyer to determine if notification requirements triggered (either in contract or under state laws).
  - Notice to state administrative agencies.
  - Notice to potentially affected persons.
  - States differ, including process and content.
- Contact criminal authorities
- Contact insurance carrier
- Call bank



Incident Response Life Cycle

IRP

- Initiate internal investigation into:
  - Cause of breach
  - Cure breach/system shutdown
  - Data affected
  - Persons affected and their locations
- Follow procedures to preserve electronic evidence.

Data Breach Event –Notices

- 47 States have breach notice laws – Not consistent
  - Might not apply to attorney-client information disclosure
  - Apply to unencrypted data
  - Timing is usually as soon as reasonable, allowing time for investigation (New Minnesota law is 48 hours!)
  - 14 States require notice to various state agencies
- Contractual Notices
  - Credit Card Processors/Banks
  - Hefty fines in the event of failure to give notice
  - Liability may exist even with notice, but failure to give notice is worse
- Client Notices: Ethical Rule 1.4 – Keep Client Informed

Basic Steps to Improve Security

- Ensure IT systems are secure and password protected.
- Protect wireless transmissions.
- Hard drives/flash drives in disposed equipment (including personal equipment) should be wiped.
- Consider computer privacy screens.
- Watch wandering eyes.
- Encrypt where possible (watch for weakest link).
- Employee training.

Thank You

Lawrence H. Kunin
Morris, Manning & Martin, LLP
1600 Atlanta Financial Center
3343 Peachtree Road, NE
Atlanta, Georgia 30326
Direct: 404.504.7798
lkunin@mmmlaw.com

Disclaimer: *The materials and information presented and contained within this document are provided by MMM as general information only, and do not, and are not intended to constitute legal advice.*

Any opinions expressed within this document are solely the opinion of the individual author(s) and may not reflect the opinions of MMM, individual attorneys, or personnel, or the opinions of MMM clients.

The materials and information are for the sole use of their recipient and should not be distributed or repurposed without the approval of the individual author(s) and Morris, Manning & Martin LLP.

This document is Copyright ©2015 Morris, Manning & Martin, LLP. All rights reserved worldwide.