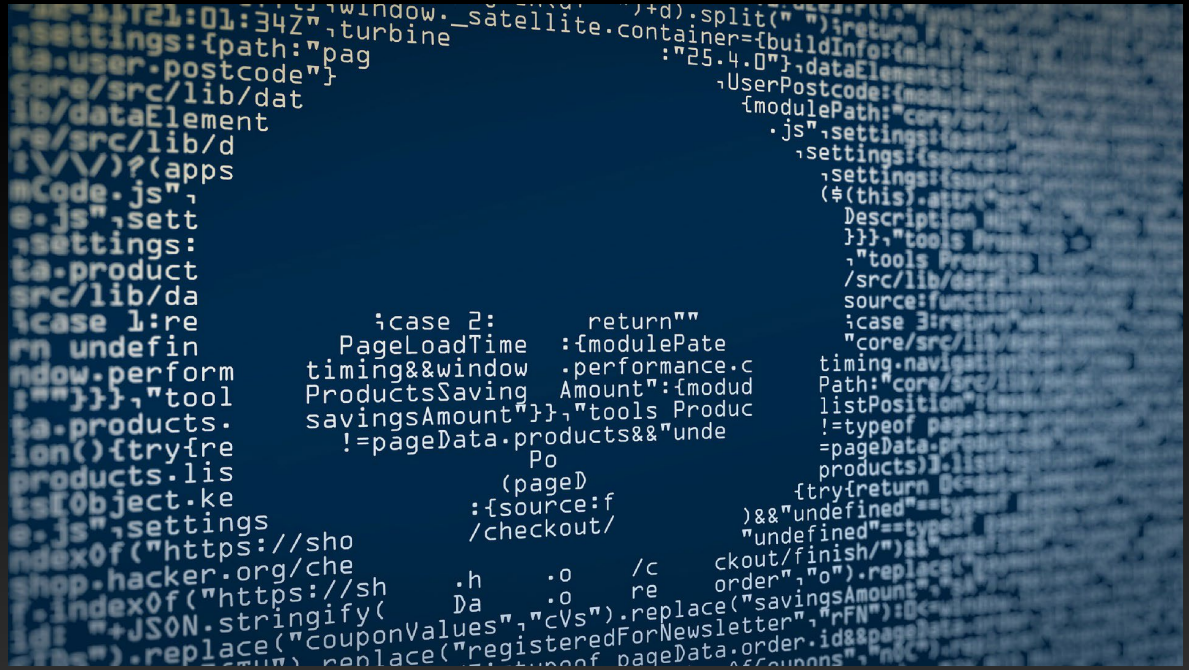
“Best Practices” for Cybersecurity, Data Privacy and Data Governance

PRESENTATION FOR FLORIDA BAR ASSSOCIATION

THIS “BEST PRACTICES” GUIDE IS INTENDED FOR EDUCATIONAL AND AWARENESS PURPOSES ONLY. IT IS NOT LEGAL ADVICE. READERS ARE STRONGLY ENCOURAGED TO RETAIN APPROPRIATE PROFESSIONALS.

RISK OF CYBERATTACKS ON LAWYERS IS GROWING



ABA ETHICS

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 483 **October 17, 2018**

A. Duty of 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*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (Emphasis added.)[9]

ABA ETHICS

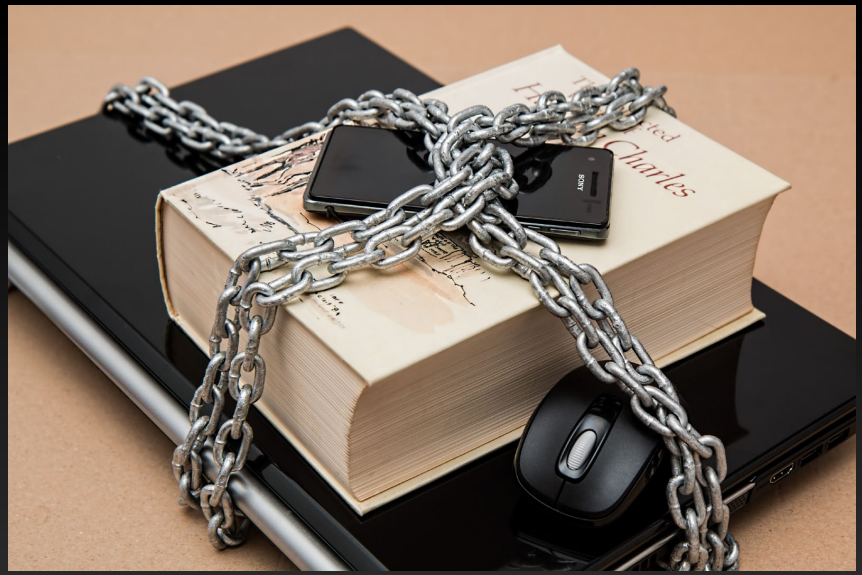
1. Obligation to Monitor for a Data Breach

Model Rules 5.1 and 5.3 impose upon lawyers the obligation to ensure that the firm has in effect measures giving reasonable assurance that all lawyers and staff in the firm conform to the Rules of Professional Conduct. Model Rule 5.1 Comment [2], and Model Rule 5.3 Comment [1] state that lawyers with managerial authority within a firm must make reasonable efforts to establish internal policies and procedures designed to provide reasonable assurance that all lawyers and staff in the firm will conform to the Rules of Professional Conduct. Model Rule 5.1 Comment [2] further states that "such policies and procedures include those designed to detect and resolve conflicts of interest, identify dates by which actions must be taken in pending matters, account for client funds and property and ensure that inexperienced lawyers are properly supervised."

Applying this reasoning, and based on lawyers' obligations (i) to use technology competently to safeguard confidential information against unauthorized access or loss, and (ii) to supervise lawyers and staff, the Committee concludes that lawyers must employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relating to data[12] and the use of data. Without such a

MEASURES TO REDUCE EXPOSURE FROM A SUCCESSFUL CYBERATTACK

- Reducing Exposure
- Personnel Education and Commitment
- Technical Measures



REDUCING EXPOSURE

REDUCING EXPOSURE

Data Identification

a) What data do I have?

b) Where is my data?

REDUCING EXPOSURE

Data Analysis

a) Do I maintain privileged client information? If yes, do I know all of the locations where privileged data rests? (personal devices, thumb drives, copiers/scanners?

b) Do I maintain third-party data that is the subject of court-ordered confidentiality agreements? If so, am I subject to contempt proceedings and/or sanctions if it is released?

REDUCING EXPOSURE

Data Analysis

c) Do I maintain emails dating back beyond a useful need?

d) Do I maintain Personally Identifiable Health Information or other information which is subject to HIPPA? If so, is this information that of your staff, your Clients, or third parties?

REDUCING EXPOSURE

Data Analysis

e) Do I maintain data that is or may be subject to other Federal laws?

f) Do I maintain data that is subject to privacy laws from a growing number of states and even international privacy laws that could subject my firm to class action lawsuits, civil penalties or mandatory reporting?

REDUCING EXPOSURE

Data Minimization – "What data do I need?"

a) Adopt and encourage compliance with internal policies that limit the collection of information. Ensure adequate enforcement of these policies.
b) Establish a data retention policy. Ensure adequate enforcement of this policy.
c) If the law firm retains case files and other client data from closed matters, consideration should be given to establishing a closed file policy. Ensure adequate enforcement of this policy.

REDUCING EXPOSURE

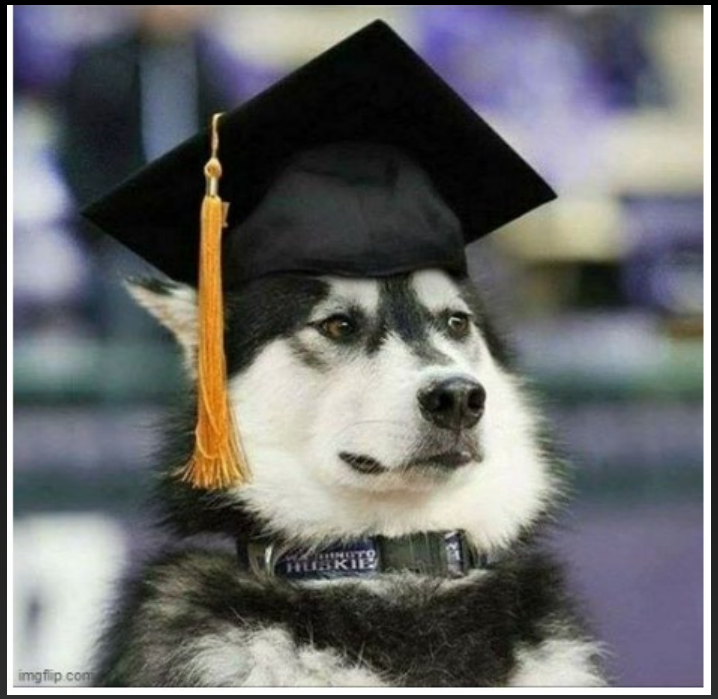
- **Data Classification**
  - ***Not all data is the same.***
  - Some data classifications to consider:
    - Business critical
    - Confidential
    - HIGHLY confidential

REDUCING EXPOSURE

- **Data Segregation**
  - Need to know basis
  - Does any particular person who has access to data really need it?
  - Are personnel and employee medical information on the same network as email?
  - Are ‘confidential’ and ‘highly confidential’ information accessible to users who do not need that access?

PERSONNEL EDUCATION AND COMMITMENT

The majority of cyber attacks are linked to our own user mistakes



- Weak passwords
- Falling for phishing scams
- Clicking on a malware infected link
- Personal devices (non-work related activity)

PERSONNEL EDUCATION AND COMMITMENT

Develop Policies and Procedures to Reduce Human Error

a) Establish a Data Governance program which is designed to provide the law firm with a holistic approach to collecting, managing, securing, and storing different types of data. The Data Governance program ought to provide for accountability, transparency, effectiveness, responsiveness, and compliance with legal and regulatory requirements.

b) Enforce the program.

PERSONNEL EDUCATION AND COMMITMENT

Educate and Inform

- Proactively educate on the organization's information security policies and procedures.
- Provide materials and resources to increase organization-wide awareness to accountability.
- Develop personnel tabletop training programs such as simulated phishing attempts, ransomware attack, or service interruption attacks.

PERSONNEL EDUCATION AND COMMITMENT

Senior Leadership Must Buy-In

- If the “boss” doesn’t demonstrate the importance of preventative and risk-reducing behavior, then neither will staff.
- Your personnel must “trust” the process. To do so, transparency between leadership and personnel concerning the law firm’s information security operation, security incidents, and commitment is paramount.

PERSONNEL EDUCATION AND COMMITMENT

Act Now. You Can't Later

- Establish an internal incident response team, clearly define each member's roles and responsibilities, and list the contact information for each member of the team.
- Conduct regular vulnerability scans and software updates on the firm's data systems to identify potential vulnerabilities and weaknesses, which are constantly being discovered.

PERSONNEL EDUCATION AND COMMITMENT

Act Now. You Can't Later

- Ensure the firm's data systems are safely backed up to reduce the risk of business interruption if the firm were victimized by ransomware. Do not backup to any accessible network as the data on the backup may become as "infected" as your other data.

- Consider obtaining cyber insurance (if available) and if obtained ensure a copy of the policy documents are stored in hard copy off the organization's system and are easily accessible if the firm loses access to its systems.

PERSONNEL EDUCATION AND COMMITMENT

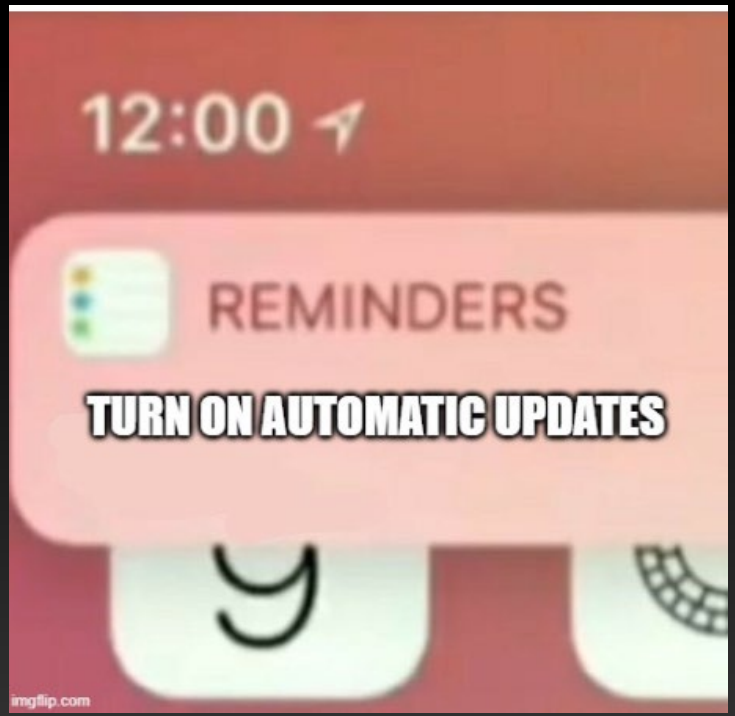
Act Now. You Can't Later

- Assess third party vendor security to ensure the vendor's practices and policies are in compliance with the firm's privacy policies, practices, and procedure. More and more, Clients are requiring that law firms certify that its vendors are also secure.

TECHNICAL MEASURES

TECHNICAL MEASURES

Automatic Updates



TECHNICAL MEASURES

Data Backups

Backups can get infected

ROUTINELY TEST
ROUTINELY TEST
ROUTINELY TEST

TECHNICAL MEASURES

Multi-Factor Authentication (MFA)

TECHNICAL MEASURES

Email, Cloud, and System Security

- Robust digital security signature

- "Front gate"
- "Back gate"
  - EDR (End-point detection & response)

FRANKLIN ZEMEL

Franklin Zemel is a partner at Saul Ewing Arnstein & Lehr, LLP and graduated from the University of Miami School of Law in 1989. He is a Certified Information Privacy Professional and his practice includes Privacy and Cybersecurity Law, Religious Land Use and First Amendment law, Complex Business Litigation and Appellate Law. Franklin represents large and small businesses, manufacturers, and religious entities in South Florida and has several significant reported cases. In addition to his state bar admissions, Franklin is admitted to practice in U.S. District Courts in the Southern and Middle Districts of Florida, the Southern District of New York and Western District of Michigan.

Saul Ewing LLP's experienced attorneys regularly consult with and assist organizations implement and establish internal privacy policies and robust incident response plans, comply with state and federal information privacy laws, and respond to and mitigate against cybersecurity incidents.