AMERICAN BANKRUPTCY INSTITUTE

2018 Annual Spring Meeting

Your Ethical Duties

Ira L. Herman, Moderator
Blank Rome LLP; New York

Bennett B. Borden
Drinker Biddle & Reath LLP; Washington, D.C.

Elizabeth B. Vandesteeg
Sugar Felsenthal Grais & Hammer LLP; Chicago

Nicolette C. Vilmos
Broad and Cassel LLP; Orlando, Fla.

ETHICS PROGRAM

2018

Protecting Client Confidences: Ethical Obligations and Best Data Security Practices

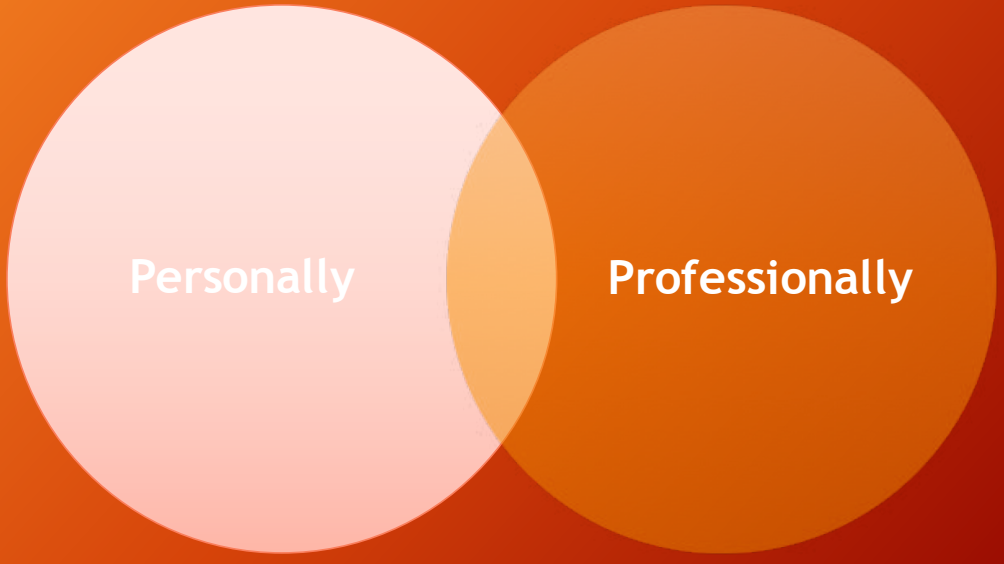
- April 19-22, 2018 Washington, DC

Ira L. Herman, Moderator
Blank Rome LLP; New York

Elizabeth ("Lisa") B. Vandesteeg
Sugar Felsenthal Grais & Hammer LLP; Chicago

Nicolette C. Vilmos
Broad and Cassel LLP; Orlando, Fla.

Why is Cyber-Security Important?



Cyberspace is a Scary Place

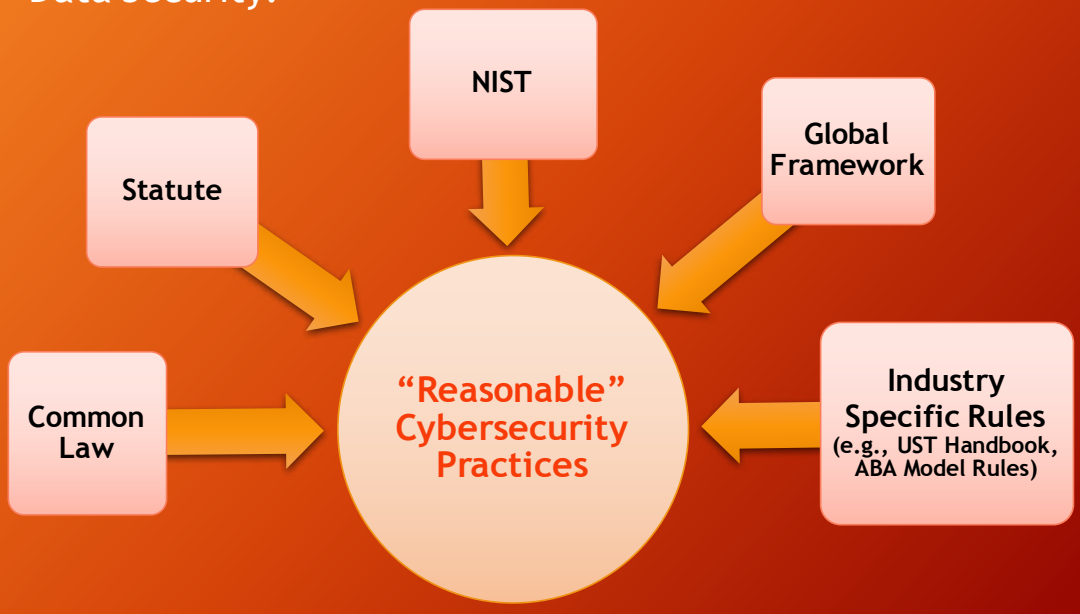
Professional Services Firms are High Quality Targets

- They are data aggregators of high quality data
- They are easy targets

What Should I Do About the Threat?

- Step 1 • Become aware of threats
- Step 2 • Analyze vulnerabilities
- Step 3 • Inventory data
- Step 4 • Understand the standard of care
- Step 5 • Meet the standard of care
- Step 6 • Develop and implement a security program

What are the Standards of Care for Insuring Data Security?



Ethical Obligations

MRPC Rule 1.1

MRPC Rule 1.6

MRPC Rule 5.3 (Cmt. 3)

Amended Model Rule 1.1

- "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."
  - Practically speaking, "[t]his provision will require lawyers to better understand any advances in technology that genuinely relate to competent performance of the lawyer's duties to a client."

The Scope of the Duty of Confidentiality

- The duty of confidentiality is far broader than the narrow duty underpinning the attorney-client privilege
  - A lawyer owes a duty of care in protecting the confidences of a client, even those of a prospective client with whom no attorney-client relationship is formed. See ABA Comm. on Ethics and Professional Responsibility, Formal Op. No. 90-358, Sept. 13, 1990.
    - *United States v. Morrell-Corrada*, 343 F Supp 2nd 80, 88 (2004).

ABA Model Rule 1.6(c)

- Imposes a duty of confidentiality, which includes protection of client information.
  - "a lawyer shall make reasonable efforts to prevent ... the unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."
- Comment 18 provides that:
  - Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, 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). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule

Limits of a Lawyer's Duties Under- Model Rule 5.3

- "A lawyer's duty is to take reasonable steps to protect confidential client information, not to become an expert in information technology," and "[w]hen it comes to the use of cloud computing, the Rules of Professional Conduct do not impose a strict liability standard."
  - The New Hampshire Bar

ABA Formal Opinion 477

- Seven factors to consider when determining the appropriate level of cybersecurity:
  - The nature of the threat.
  - How client confidential info is stored and sent
  - The use of reasonable electronic security measures.
  - How electronic communications should be protected.
  - The need to label client information as privileged and confidential.
  - The need to train lawyers and nonlawyer assistants.
  - "The need to conduct due diligence on vendors who provide technology services. Guidance in this regard can be found in ABA Formal Opinion 08-451.

ABA Formal Opinion 477
https://www.americanbar.org/content/dam/aba/images/abanews/FormalOpinion477.pdf

Adapting to New Technologies

Professionals must inform themselves of the risks of inadvertent or unauthorized disclosure of client's cyber data and take reasonable and information-appropriate measures to reduce those risks

What Technology Is Implicated

- Computers, tablets, smart phones, scanners, printers or copiers. This category also includes the use of email, and the electronic storage of documents and other information.
- Programs for compiling, storing, and reviewing electronically-stored information (ESI). Law firm management and administration software, designed to integrate various facets of client information, contacts, time entry, billing, document management, docketing and calendaring, and/or other CRM functions.
- Technology clients are using and how that technology impacts their business.
- Technology that could be used to impose liability on clients, such as, for example, GPS technology, electronic logging, or automated driving technology in the context of personal injury suits caused by car accidents.
- Technology that can be used in courtrooms is critical.
- Data security fundamentals as to what steps can be taken to keep that data (belonging to either the firm or a client) protected.

Extra Security Measures are Appropriate

- Compliance with minimum standards of any kind--including those delineated in ethics rules--should only be a starting point for effective cybersecurity practice"
    - The ABA Cybersecurity Handbook

It's Not Just the Law Firm Anymore

- "To reflect the scope of the nonlawyer services now being provided outside of firms," Model Rule 5.3's commentary now references "cloud computing" as an example of modern outside help.

Supervising Third Parties

- A law firm's data security practices are only as strong as its weakest link
- Lawyers must make sure that law firm staff and external business partners understand necessary data security practices and the critical role all parties play in ensuring the protection of client information

Client Audits

- Clients (especially in highly regulated industries) are insisting that their lawyers take appropriate measures to protect proprietary, regulated, or confidential information

Personally Identifiable Information (PII)

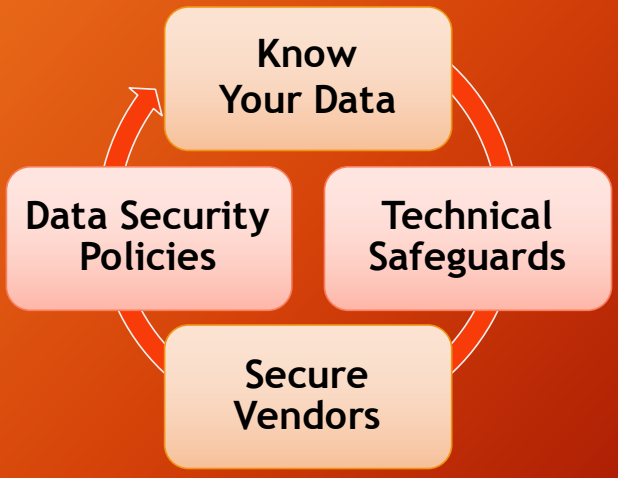
- Safeguarding personally identifiable information in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public
  - OMB memorandum Safeguarding Against and Responding to the Breach of Protecting Personally Identifiable Information (May 22, 2007)

What is a Data Breach?

- Definition varies from state to state, but typically includes:
  - Unauthorized acquisition/access/use
  - Of Personally Identifiable Information (PII)
  - Unencrypted
  - Compromising the security, confidentiality or integrity of PII
  - Does not include good faith acquisition of PII

20

Protecting Valuable Client Information



Why We Should Be Careful Using the "B" Word

- Using "breach" to describe a data-privacy related incident assumes the incident meets the definition of a security breach which triggers various notification requirements
- An "incident" does not always rise to the level of "breach" (i.e., encryption safe harbor)
- "Incident" is better received by the public than "breach"

Breach & Breach Reporting

What is a breach?	How does a breach occur?	Now what?
• Hacking • Phishing • Malware • Theft • Misuse	• Motive • Opportunity • Weak security • Weak policies	• Respond quickly • Respond appropriately • Preserve evidence

Who Should Be On Your Incident Response Team?

- Because the issue impacts almost every component of the organization, and failure to properly manage can result in both long and short term consequences, the team should include "C" level decision makers in the following areas:
  - Legal
  - IT
  - Risk management/insurance
  - HR
  - Marketing
  - Public relations
  - Compliance & internal audit
  - Physical security
  - Other executive, as appropriate
  - Third party response services (e.g., forensics, privacy counsel, notification)

Steps in a Breach Response

Discovery & Reporting	• Identify the incident or potential incident. • Immediately report the incident or threat to the proper party.
Initial Response	• Secure and isolate affected systems to limit further data loss. • Preserve evidence. Convene the Incident Response Team in accordance with this Plan. • Know your role. Coordinate investigation and remediation.
Investigation	• Gather information on the incident. • Consider involving forensics team and outside counsel. • Analyze the cause of the incident and the affected systems. • Analyze legal requirements and liabilities going forward.
Remediation	• Comply with legal requirements including breach notification. • Remove known vulnerabilities; repairing systems. • Respond to third party inquiries. Consider contacting law enforcement.
Post-Incident Review	• Review analysis and notes regarding the incident. • Improve practices as necessary. • Improve policies as necessary.

Cybersecurity extends beyond computers

- How can you protect yourself?
- Remember physical security – Having physical access to a device makes it easier for an attacker to extract or corrupt information. Do not leave your device unattended in public or easily accessible areas.
- Keep software up to date – If the vendor releases updates for the software operating your device, install them as soon as possible. Installing them will prevent attackers from being able to take advantage of known problems or vulnerabilities.
- Use good passwords – Choose devices that allow you to protect your information with passwords. Select passwords that will be difficult for thieves to guess, and use different passwords for different programs and devices. Do not choose options that allow your computer to remember your passwords.
- Encrypt files – If you are storing personal or corporate information, see if your device offers the option to encrypt the files. When you use encryption, it is important to remember your passwords and passphrases; if you forget or lose them, you may lose your data.

Securing Wireless Networks

- Be cautious of public Wi-Fi networks – Before you connect to any public wireless hotspot—like on an airplane or in an airport, hotel, train/bus station:
  - Be sure to confirm the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate.
  - Do not conduct sensitive activities, such as online shopping, banking, or sensitive work, using a public wireless network.
  - Only use sites that begin with "https://" when online shopping or banking. Using your mobile network connection is generally more secure than using a public wireless network.

Smartphone Security

- Set PINs and passwords.
- Do not modify your smartphone's security settings.
- Backup and secure your data.
- Only install apps from trusted sources.
- Understand app permissions before accepting them.
- Use the free, built-in security features.
- Accept updates and patches to your smartphone's software.
- Wipe data on your old phone before you donate, resell, or recycle it.
- Report a stolen smartphone.

https://www.fcc.gov/smartphone-security

Bluetooth Security

- If someone can "discover" your Bluetooth device, they may be able to send unsolicited messages which could cause you to be charged extra fees and they may be able to find a way to access or corrupt your data.
- Disable Bluetooth when you are not using it - Unless you are actively transferring information from one device to another, disable the technology to prevent unauthorized people from accessing it.
- Use Bluetooth in "hidden" mode - When you do have Bluetooth enabled, make sure it is "hidden," not "discoverable." The hidden mode prevents other Bluetooth devices from recognizing your device. This does not prevent you from using your Bluetooth devices together.
- Be careful where you use Bluetooth - Be aware of your environment when pairing devices or operating in discoverable mode. For example, if you are in a public wireless "hotspot," there is a greater risk that someone else may be able to intercept the connection than if you are in your home or your car.

Risky Business for Bankruptcy Counsel

30

Property of the Estate I

- Upon the filing of a bankruptcy petition, the bankruptcy estate is created from the Debtor's property
- Section 541 of the Bankruptcy Code defines what property is included in and excluded from a debtor's bankruptcy estate. See 11 U.S.C. § 541(a)-(f)

Property of the Estate II

- The bankruptcy estate is the pool of assets that is subject to the jurisdiction of the bankruptcy court and from which creditors' claims are paid
- Electronically stored proprietary information can be the most valuable "property of the estate" in many bankruptcy cases

The United States Trustee's Handbook Requirements– Guidance For All of Us

- Chapter 7 trustees must comply with guidelines:
  - imposing specific restrictions on the use of wire transfers
  - requiring specific computer security measures
  - requiring trustees to develop and maintain a business interruption plan
  - requiring specific records security and retention policies, including individual case records and tax returns
    - The United States Trustee's Handbook for Chapter 7 Trustees (pages 5-15 to 5-21)

Client Counseling Issues

- The Chapter 7 Trustee or the DIP have fiduciary duties to creditors and other parties in interest
- As a lawyer – what are you client counseling obligations?
- Breach insurance
- Employee policies
- ESI preservation in contemplation of litigation

Resources

- "The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals, Second Edition"
- National Cyber Security Alliance (NCSA) - https://staysafeonline.org/about/
- US-CERT – United States Computer Emergency Readiness Team- https://www.us-cert.gov/