Spies, Crimes, and Ethical Lines: Practical Cybersecurity for Attorneys

Jon Knight

BakerHostetler

I. Introduction & Framing the Risk

Objectives

- Understand cybersecurity as an **ethics + malpractice + regulatory issue**
- Recognize law firms as **high-value targets** (IP, M&A strategy, privileged communications)

Key Points

- Law firms are "prime targets" for cyberattacks due to access to sensitive client data
- Threat actors include **criminal groups and nation-states** seeking litigation strategy or insider trading info

Transition: Cybersecurity is not just IT—it is governed by core ethics rules.

II. Core Ethical Duties Under the ABA Model Rules

A. Duty of Competence – Rule 1.1 (incl. Comment 8)

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

[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 relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."

ABA Formal Opinion 477R further explains this comment:

"Model Rule 1.1 requires a lawyer to provide competent representation, and Comment [6] [renumbered as Comment [8]] specifies that, to remain competent, lawyers need to "keep abreast of changes in the law and its practice." The Commission concluded that, in order to keep abreast of changes in law practice in digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today's environment without knowing how to use email or create an electronic document."

Key take aways

- Requires "competent representation"
- Comment 8: lawyers must understand **risks and benefits of relevant technology**
- These rules are adopted in **most U.S. jurisdictions (~40+ states)**

Teaching Point:
Cybersecurity competence is affirmative—not delegable to IT vendors. This means that even lawyers who are not "techy" must have a basic understanding of relevant technology, and that relevant technology includes cybersecurity.

B. Duty of Confidentiality – Rule 1.6

"(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."

- Requires "reasonable efforts" to prevent unauthorized disclosure
- Comment 18 explains what are reasonable efforts.
    - "The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client 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, 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)."
- **ABA Formal Opinion 477R further explains this comment:**

"What constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors. In turn, those factors depend on the multitude of possible types of information being communicated (ranging along a spectrum from highly sensitive information to insignificant), the methods of electronic communications employed, and the types of available security measures for each method."

- In other words, lawyers are allowed to weigh certain pros and cons when considering if their security efforts are "reasonable."
    - How sensitive is the data? More sensitive data (e.g., SSNs, financial account information, health or medical information) likely requires more safeguards in order to protect confidentiality.
    - What is the likelihood of disclosure if I do not implement the safeguard?

- Cost vs. burden of safeguards – if I am a solo practitioner, I obviously do not have the same budget for IT and cybersecurity as a large firm so should not necessarily have the same safeguards.

- Remember: what constitutes reasonableness may also include outside counsel guidelines you agree to as part of the representation.

C. Duty to Communicate – Rule 1.4

- "reasonably consult with the client about the means by which the client's objectives are to be accomplished."

- **ABA Formal Opinion 477R further explains this comment:**

"When the lawyer reasonably believes that highly sensitive confidential client information is being transmitted so that extra measures to protect the email transmission are warranted, the lawyer should inform the client about the risks involved."

-

C. Supervision Duties – Rules 5.1 & 5.3

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."

- How does this apply to cybersecurity and technology?

ABA Formal Opinion 483 gives the answer. "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 and the use of data…. Thus, just as lawyers must safeguard and monitor the security of paper files and actual client property, lawyers utilizing technology have the same obligation to safeguard and monitor the security of electronically stored client property and information."

Key Risk Insight based on the ABA Opinion:
Supervisory lawyers may be liable for cybersecurity failures of staff or vendors. "The potential for an ethical violation occurs when a lawyer does not undertake reasonable efforts to avoid data loss or to detect cyber-intrusion, and that lack of reasonable effort is the cause of the breach."

III. I have had a cyber incident: what are my obligations? ABA Formal Opinion 483 again has the answer.

1. "Promptly to stop the breach and mitigate damage resulting from the breach."

How do I do this? The ABA Opinion does NOT have the answer.

- "**How a lawyer does so in any particular circumstance is beyond the scope of this opinion."**
- It does however, heavily suggest that failure to have a plan for how you will respond to a cybersecurity incident could be considered unreasonable.
    - "As a matter of preparation and best practices, however, lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach."

2. Determine what occurred

- According to Opinion 483, "A post-breach investigation requires that the lawyer gather sufficient information to ensure the intrusion has been stopped and then, to the extent reasonably possible, evaluate the data lost or accessed."

3. Evaluate obligations to notify clients and individuals

- ABA Opinion 483: "When a data breach occurs involving, or having a substantial likelihood of involving, material client confidential information a lawyer has a duty to notify the client of the breach."
    - This notice obligation does not extend to former clients: "The Committee is unwilling to require notice to a former client as a matter of legal ethics in the absence of a black letter provision requiring such notice."

- Applicable state law
    - Every state in the United States and four U.S. territories have enacted laws requiring notification in the event of a data security breach. The law applicable to a given individual is the law of his or her state of residence, not the law of the state in which the entity that experienced the breach is located. If an incident involves individuals who reside in multiple states, the incident response will be governed by more than one state law.
    - The majority of the data breach notification laws require notification if there is a security breach involving the unauthorized acquisition of personal information.
        - Alabama, Alaska, Arkansas, California, Colorado, Delaware, D.C., Georgia, Idaho, Illinois, Indiana, Iowa, Kentucky, Maine, Maryland, Massachusetts, Minnesota, Mississippi, Montana, Nebraska, Nevada, New Hampshire, New Mexico, North Dakota, Oregon, South Dakota, Tennessee, Texas, Utah, Vermont, Virgin Islands, Washington, Wisconsin, and Wyoming.

- Five other states and one territory require notification if there is a security breach that involves unauthorized access to personal information.
    - Connecticut, Florida, New Jersey, New York, Rhode Island, and Puerto Rico. Connecticut, New York, and Rhode Island require notification if there is unauthorized access to or unauthorized acquisition of personal information.
- Several other states and territories require both access to and acquisition of personal information to constitute a breach requiring notification.
    - Arizona, Guam, Hawaii, Kansas, Louisiana, Michigan, Missouri, North Carolina, Ohio, Oklahoma, Pennsylvania, South Carolina, Virginia, and West Virginia.
- While the definition of "personal information" varies amongst the states, "personal information" generally is defined as an individual's name in combination with the individual's Social Security number, driver's license number, or financial account number. Many state laws expound on these core elements of personal information to include additional data sets, such as medical information, health insurance number, passport number, maiden name, and/or full date of birth. Additionally, some data security breach notification statutes require an entity to notify state regulatory authorities, including state attorneys general, and have varying numerical thresholds that trigger an entity's regulatory notice obligations.

Example: Virginia (Va. Code § 18.2-186.6)

- Definition of Personal Information An individual's first name or first initial and last name in combination with and linked to any one or more of the following: • Social Security number; • Driver's license number or state identification card number issued in lieu of a driver's license number; • Financial account number or credit card or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial accounts; • Passport number; or • Military identification number.
- In addition to notifying individuals without unreasonable delay, if any Virginia resident is notified, you must also notify the Attorney General of Virginia.

Check Your Engagement Letters or Other Applicable Legal Regimes

- In addition to custom notice obligations included in outside counsel guidelines or engagement letters, laws and regulations such as HIPAA, banking regulations, insurance regulations, government contracting, etc. may have other notice obligations.

IV. State Bar Variations & Emerging Standards

A. California (Formal Opinion 2020-203)

- This opinion emphasizes that the firms should likely undertake a risk assessment as part of determining the reasonableness of its cybersecurity measures under Rule 1.1
    - "Part of the risk assessment process should include reasonable efforts to ensure that all firm members appreciate the risks involved in keeping confidential client information on electronic systems and the steps that the firm's managers have implemented to minimize the risk of unauthorized disclosure. Because the risk-assessment process is on-going, particularly with the introduction of new technologies and new threats, this duty would require managers and supervisors to establish ongoing and evolving protective measures with respect to the use of its technology, and regularly monitoring the same, and to keep subordinate lawyers and staff up to date as new measures are implemented."
    - ---

B. New York (Formal Opinion 2024-3)

- Provides important clarity when handling ransomware attacks.
    - "There is no ethical prohibition against, or requirement to, pay a ransom to a cyber extortionist, and lawyers and law firms may be not candid with respect to certain material facts when negotiating with cyber-extortionists in efforts to protect or regain access to client information and firm systems."

C. Cross-Jurisdiction Themes

- "Reasonable security" standard (fact-specific)
- Broad adoption of tech competence
- Increasing focus on:
    - Incident response planning
    - Vendor management
    - Client notification obligations

D. Practical CLE Note (for audience)

Differences are less about *whether duties exist* and more about **how aggressively enforced and interpreted**

VI. Tabletop Exercise (Nation-State Law Firm Breach)

Scenario Overview

Your firm represents:

- Public companies in active M&A deals
- Defense contractor clients

Incident:

- Nation-state APT gains access via compromised vendor
- Exfiltrates:
    - Draft merger agreements
    - Defense procurement documents

Exercise Structure

Phase 1: Detection & Initial Response

Questions:

- What triggers ethical duties under Rule 1.1 and 1.6?
- Who is on the incident response team?
- What are your **first 3 actions within 24 hours?**

Phase 2: Scope & Investigation

Questions:

- How do you determine:
    - What data was accessed?
    - Which clients are impacted?
- What is “reasonable investigation” under ABA 483?

Phase 3: Client & Regulator Notification

Decision Points:

- Which clients must be notified?
- Timing of disclosure under Rule 1.4
- Do you:

- Notify law enforcement?
- Coordinate with national security agencies?

Phase 4: Strategic & Ethical Tensions

Issues:

- Client confidentiality vs. cooperation with government
- Conflicts if firm's negligence is implicated
- Continued representation vs. withdrawal

Facilitator Debrief

Tie back to:

- Rules 1.1, 1.4, 1.6
- ABA 483 lifecycle obligations
- State bar obligations (NY/CA)

VII. Key Takeaways & Practical Checklist

A. Ethics = Cybersecurity Governance

- Not just IT—board/partner responsibility

B. Minimum Defensible Posture

- Risk assessment
- Written incident response plan
- Vendor oversight program
- Training + phishing awareness

C. Litigation Reality

- Breach ≠ violation
- **Failure to take reasonable steps = violation**