JENNER&BLOCK

CLE RELAY

The Ethics of Cybersecurity Before, During, And After an Incident

John Storino, Shoba Pillay &
Lindsey Lusk

Poll Question

What are a lawyer's ethical obligations with respect to cybersecurity?

(a) Every lawyer in the organization must have a complete understanding of the entity's cybersecurity protocols.

(b) None. That is the role of our IT staff.

(c) I would rather get sanctioned by the bar than deal with cybersecurity.

(d) The IT staff must be adequately supervised by an attorney who has a working knowledge of cybersecurity.

Agenda

- Lawyers' professional obligations
- Importance of preparation before an incident
- How to respond to a cybersecurity incident
- Next steps in incident response
- Privilege and investigations
- Potential solutions to address privilege concerns

Lawyers' Professional Obligations

Rules Implicated

- Model Rule 1.1 – Duty of Competence
- Model Rule 5.3 – Duty to Supervise
- Model Rule 1.6 – Duty of Confidentiality
- Model Rule 1.4 – Duty of Reasonable Communication

Lawyers' Professional Obligations

Model Rule 1.1 – Duty of Competence

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

Lawyers' Professional Obligations

Model Rule 1.1 – Duty of Competence cmt. 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.

Lawyers' Professional Obligations

Duties in the Cybersecurity Space

- You can rely on qualified, competent IT professionals to satisfy the duty of competence in the cybersecurity space

- ABA Formal Op. 483:

> "A competent lawyer must use and maintain those technologies in a manner that will reasonably safeguard property and information that has been entrusted to the lawyer. A lawyer's competency in this regard *may be satisfied either through the lawyer's own study and investigation or by employing or retaining qualified lawyer and nonlawyer assistants"* (emphasis added)).

- Are your IT people qualified?

- But don't forget about Rule 5.3

Lawyers' Professional Obligations

Model Rule 5.3 – Duty to Supervise

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

(a) a partner, and a lawyer who individually or together with other lawyers possesses comparable 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;

(b) 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; . . . .

Lawyers' Professional Obligations

Duties in the Cybersecurity Space

- Need to have "reasonable measures" of supervision in place
  - Don't have to become an expert
- Concrete steps to take to comply
  - Monthly meetings
  - Written policies
  - Regular evaluations
- Proper infrastructure to ensure proper supervision
  - Full-time, trained, and qualified IT staff
  - Director of IT
  - Reporting structure to management
  - Supplement with third-party vendors specializing in IT

Lawyers' Professional Obligations

Model Rule 1.6 – Duty of Confidentiality

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

. . . .

(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.

Lawyers' Professional Obligations

Duties in the Cybersecurity Space

- Must make "reasonable efforts" to secure information
- "Reasonable" or "Reasonably," when used in relation to a lawyer's conduct, "denotes the conduct of a reasonably prudent and competent lawyer." ABA Model Rule 1.0(h)
- Fact-based inquiry that depends on the circumstances
  - Consider what safety measures are industry-standard
  - It's an evolving standard
- Concrete steps to comply
  - Multi-factor authentication
  - Encryption
  - Physical security of devices

Lawyers' Professional Obligations

Model Rule 1.4 – Duty of Reasonable Communication

(a) A lawyer shall:

(1) promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(e), is required by these Rules;

(2) reasonably consult with the client about the means by which the client's objectives are to be accomplished;

(3) keep the client reasonably informed about the status of the matter;

(4) promptly comply with reasonable requests for information; and

(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

Lawyers' Professional Obligations

Duties in the Cybersecurity Space

- Ensure proper reporting to management
- Disclosing a cybersecurity incident
  - "[T]he inherent uncertainty often surrounding cyberattacks means that Rule 1.4(b)'s admonition for lawyers to 'explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation' may not be triggered because the impact on the matter at hand may be less than clear to the lawyer."

Eli Wald, *Legal Ethics' Next Frontier: Lawyers and Cybersecurity,* 19 Chap. L. Rev. 501, 534 (2016)

Lawyers' Professional Obligations

Duties in the Cybersecurity Space

- Disclosing a cybersecurity incident
  - "The information gathered in a post-breach investigation is necessary to understand the scope of the intrusion and to allow for accurate disclosure to the client consistent with the lawyer's duty of communication and honesty under Model Rules 1.4 and 8.4(c)."

    ABA Formal Op. 483

  - State ethics opinions consistently hold that notification must be timely once the attack is understood.

  - Best practice is to advise management right away (even if you don't have a complete picture) and then update them as necessary

Agenda

- Lawyers' professional obligations
- Importance of preparation before an incident
- How to respond to a cybersecurity incident
- Next steps in incident response
- Privilege and investigations
- Potential solutions to address privilege concerns

Importance of Preparation Before an Incident

Preparedness is Key

- Written Plans (because your system may be inaccessible)
  - WISP = Written Information Security Plan
  - IRP = Incident Response Plan
  - DRP = Disaster Recovery Plan
  - COOP = Continuing Operations Plan

- Technical Preparation
  - Network segmentation
  - Cadence of backups
  - Patch protocol
  - Timeline to restore backups

- Designated Response Team

Importance of Preparation Before an Incident

Preparedness is Key

- Executive Buy-In:
  - Stakeholders and Executive Leadership
  - Decision Tree
  - Understand financial and organization consequences

- Practice:
  - Table-Top Exercises
    - Include Executive Leadership and Legal
    - Consider how the IRP, DRP, and COOP work together
    - Pressure test multiple scenarios
    - Develop muscle memory
  - Red Team Exercises for IS/IT Teams
  - All potential scenarios depending on business (stolen laptop, phishing, vulnerability compromise)

Importance of Preparation Before an Incident

Preparedness is Key

- Training
  - Computer Security Awareness (physical and technical)
  - Anti-Phishing
  - Culture of Security

- Pre-existing relationships with law enforcement
  - FBI

Agenda

- Lawyers' professional obligations
- Importance of preparation before an incident
- How to respond to a cybersecurity incident
- Next steps in incident response
- Privilege and investigations
- Potential solutions to address privilege concerns

How to Respond to a Cybersecurity Incident

First 24 Hours After Cybersecurity Incident

- Execute Incident Response Plan
  - Inform Executive Leadership and Board as detailed in IRP
  - Take compromised systems offline if possible
  - Execute DRP and COOP as appropriate

- Engage Support Team:
  - Outside Counsel
  - Cybersecurity forensic vendor
  - Strategic Communications

How to Respond to a Cybersecurity Incident

First 24 Hours After Cybersecurity Incident

- Consider Risks and Mitigation
  - Business risk: operating with impaired service/functionality or system downtime
  - Recovery risk: process, cost, and timing for recovery and resuming business operations
  - Litigation risk: class actions, regulatory and enforcement actions, privilege issues
  - Reputational risk: how does this impact decision making, communications approach

Agenda

- Lawyers' professional obligations
- Importance of preparation before an incident
- How to respond to a cybersecurity incident
- Next steps in incident response
- Privilege and investigations
- Potential solutions to address privilege concerns

Next Steps in Incident Response

Next Steps

- Incident-Specific Considerations
  - Ransomware:
    - Communicate with threat actor?
    - Pay ransom?
    - Factors include threat actor's reputation, impact to business for failing to pay, financial risks, sanctions risk
  - DDOS
    - Restoring customer portals
    - Reputation and customer-driven communications
  - Phishing / Social Engineering:
    - Remediate impact of phishing email
    - Educate employees

Next Steps in Incident Response

Next Steps

- Internal Business Needs
  - Remediate compromised systems
  - Resume business operations
  - Consider internal communications to manage employees

- Disclosures
  - Law enforcement
  - CISA
  - SEC
  - State notifications rules (50 state regime)

Next Steps in Incident Response

Next Steps

- Prepare for Litigation and Enforcement Actions
  - Retain all relevant logs
  - Employ litigation holds

- Lessons Learned
  - Assess what worked and what didn't
  - Improve plans and systems based on lessons learned

Agenda

- Lawyers' professional obligations
- Importance of preparation before an incident
- How to respond to a cybersecurity incident
- Next steps in incident response
- Privilege and investigations
- Potential solutions to address privilege concerns

Privilege and Investigations

Poll Question

- The chances of not having to produce the post-incident forensic report are best characterized as:
  - (a) Coin flip
  - (b) Depends on the judge
  - (c) No way in hell
  - (d) You have a fighting chance if you take the right steps

Privilege and Investigations

How do you protect a post-incident forensic report?

Attorney-Client Privilege

- Elements
  - (i) a communication
  - (ii) made between counsel and client
  - (iii) in confidence
  - (iv) for the purpose of seeking, obtaining or providing legal assistance to the client.
- Attorney-Client Privilege will likely not protect forensic reports
  - Key pitfall is the **purpose** of a post-incident investigation: often considered business purpose to get to the forensic expertise as opposed to the legal guidance

Privilege and Investigations

How do you protect a post-incident forensic report?

Work-Product Doctrine

- Elements
  - (i) Documents and tangible things;
  - (ii) Prepared in anticipation of litigation or trial; and
  - (iii) By or for the party or by or for the party's representative
- Work-Product Doctrine is a closer call

Privilege and Investigations

How do you protect a post-incident forensic report?

<u>Turning Tides</u>

- Historically, case law shows that post-incident forensic reports were often protected but recent case law suggests courts are changing their approach

Privilege and Investigations

Case Study: *In re Rutter's Data Security Breach Litigation*

- Dispute over the whether a post-incident forensic report was protected
- Arguments for Work-Product Doctrine
  - Primary motivation was anticipation of litigation
- Arguments for Attorney-Client Privilege
  - Primary purpose was to obtain legal advice or provide legal counsel with facts

Privilege and Investigations

Case Study: *In re Rutter's Data Security Breach Litigation*

- Court's ruling
  - Work Product
    - Primary motivation was not in anticipation of litigation
      - Description of Statement of Work showed business purpose
      - Corporate deponent admitted he did not anticipate litigation
      - No evidence report provided to outside counsel

Privilege and Investigations

Case Study: *In re Rutter's Data Security Breach Litigation*

- Court's ruling
  - Attorney-Client Privilege
    - Primary purpose was not for legal advice
      - Statement of Work description
      - Report set forth facts rather than presenting opinion and "tactics"
      - Extensive collaboration between IT professionals and forensic investigators
        - No involvement from legal

Privilege and Investigations

Public Relations Consultants

- No privilege where purpose of PR consultants' communications are reputational protection rather than legal defense
  - But privilege where PR consultants assist counsel
- Disclosing privilege communications to PR consultants may waive privileged
- Privilege only applies to PR consultant communication if they were essential to providing legal advice
- Another defense to disclosure of communications with PR consultant – relevance

Agenda

- Lawyers' professional obligations
- Importance of preparation before an incident
- How to respond to a cybersecurity incident
- Next steps in incident response
- Privilege and investigations
- Potential solutions to address privilege concerns

Potential Solutions to Address Privilege Concerns

Potential Solutions to Protect Forensic Reports

- Consider the substance of the Statement of Work
- Heavily involve your legal department
- Communicate orally during course of investigation
- Limit the forensic report to the findings of facts
- Prioritize getting the report to the legal department
- Have results and recommendations from the forensic investigation communicated orally