# Cyber Ethics: The Crossroads of Cybersecurity & Ethics

Presented By:

**David J. Walton**

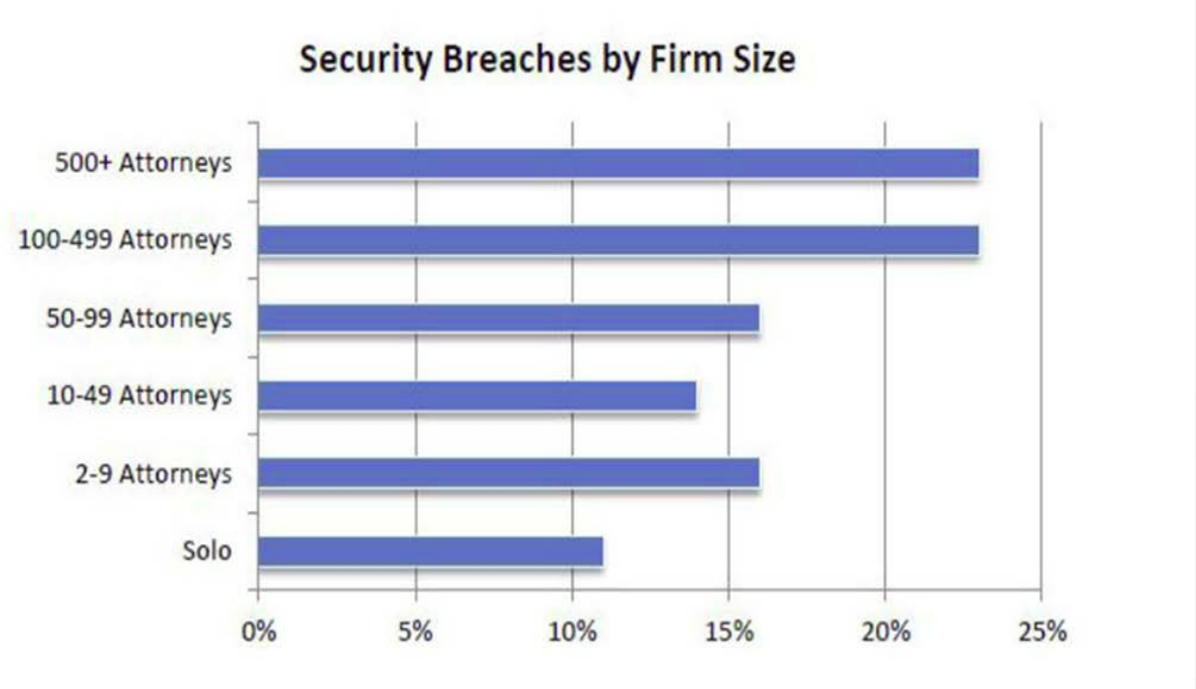
**PBI Estate Law Institute**

**November 2, 2018**

COZEN O'CONNOR

# Who Is At Risk

- Large and small firms
- Solo practitioners
- Law firms are the 7th most vulnerable industry to malware.



# Recent Developments

- Some clients are denying business to law firms that are not taking appropriate steps to manage network security risks.


- 23 NYCRR 500: third-party service vendors (law firms) must meet minimum cybersecurity practices to do business with covered entities. Vendors must contractually warrant various risk management procedures (i.e., access controls, incident response controls, encryption).

COZEN O'CONNOR

# Who Are The Perpetrators

- Social engineers (“hacktivists”)
- State-sponsored hackers
- Government intrusion and surveillance
- Criminals engaged in corporate espionage and financial crimes
- Unintentional insiders: configuration mistakes, lost equipment, etc.
- Malicious insiders
  - Current employees
  - Former employees

COZEN O'CONNOR

# Methods of Attack

- Social engineering: manipulating people to perform actions or divulge confidential information
  - Pretexting, baiting, probing, tailgating, shoulder surfing, vishing, and phishing

COZEN O'CONNOR

# Methods of Attack

- Phishing: attempt to acquire sensitive information such as usernames, passwords, and credit card details by posing as a trustworthy entity. Form of social engineering.
- Whaling: attempts on higher-net-worth or high-profile individuals.
- Generally via email or text.


COZEN O'CONNOR

# Methods of Attack


- Malware – short for malicious software
- Types include:
  - Ransomware (CryptoWall)
  - Viruses
  - Trojans
  - Worms
  - Rootkits
  - Backdoors
  - Keyloggers
  - Adware
  - Spyware
  - Scareware
  - Juice jackers

COZEN O'CONNOR

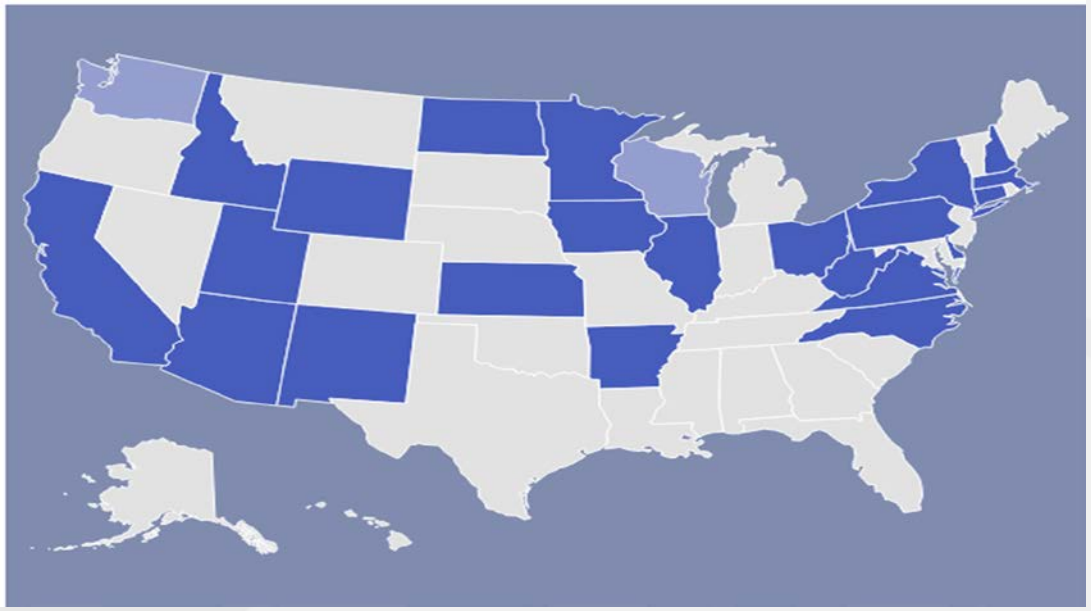
# Methods of Attack

- Ransomware: hackers hold data hostage in efforts to extort a ransom from a firm or its clients.
- Cyber criminals threaten to leak data to the public which would lead to reputational harm, business losses, etc.
- Law firms are attractive targets given the confidential, sensitive, and life or death nature of client/patient data.


COZEN O'CONNOR

# Rule 1.1 Competence

- Comment 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.”
- 26 states have adopted ABA Model Rule 1.1.



COZEN O'CONNOR

# Rule 1.6 Confidentiality

- Changes made to the ABA Rules in response to technological changes impacting the practice of law.
- 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.”


COZEN O'CONNOR

# Rule 1.6 Confidentiality

- Comment 18: requires lawyers to act competently to safeguard information relating to client representation against unauthorized access by 3rd parties and inadvertent or unauthorized disclosure by the lawyer.

- "Reasonable Efforts"
  - Sensitivity of the information
  - Likelihood of disclosure if additional safeguards are not employed
  - Comment 19
- Safeguards
  - Cost
  - Difficulty of implementing
  - Extent to which they adversely affect lawyer's ability to represent clients

COZEN O'CONNOR

# “Confidential Nature of Work” [sample firm rule]

A law firm’s work is of a confidential nature and, consequently, all work of the office should be considered confidential by the entire staff and not be discussed with others.

Care must be exercised in public areas (such as the reception area, hallways, elevators, rest rooms and the like), or at any other place where non-members of our staff may be present, not to discuss or inquire about clients’ affairs.

Firm matters should not be discussed with anyone outside the office at times or places where the conversation may be overheard by non-members of our staff.

These limitations are intended to have the broadest application and the most scrupulous attention. At times, disclosure of the mere fact the firm represents a particular client, or is working or interested in a particular property or situation, may be prejudicial to the client’s interest, and should be avoided.

Proofreading should not be done in public areas.

COZEN O’CONNOR

# Competence & Confidentiality

- Rules 1.1 and 1.6, together, require lawyers to act competently and utilize reasonable measures to protect client data and information
- Duties cover all aspects of technology
  - Phones, laptops, tablets, networks, outsourced technology, cloud computing

COZEN O'CONNOR

# Rule 1.4 Attorney-Client Communications

- Rule 1.4(a)(1): “[a] lawyer shall promptly inform the client of any decision or circumstance with respect to which the client’s informed consent…is required.”
- Does not independently require lawyers to communicate with clients regarding cybersecurity.

COZEN O’CONNOR

# Rule 1.4 Attorney-Client Communications

- Rule 1.4(a)(3): “[a] lawyer shall keep the client reasonable informed about the status of the matter.”
- Comment 3: “(a)(3) requires that the lawyer keep the client reasonably informed about…significant developments affecting the timing or the substance of the representation.”
- Rule 1.4(b): “[a] lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.”

COZEN O'CONNOR

# Attorney-Client Privilege & Work Product Doctrine

Elements:

- Privilege can be a common law or statutory or a hybrid development in a particular state such as Pennsylvania.
- The attorney-client privilege protects confidential communications between client and lawyer made for the purpose of obtaining or providing legal assistance
- Argument against the protection provided by the attorney-client privilege is that it hinders access to the truth
- However,
  - Privilege is generally construed as narrowly as possible
  - Burden rests on party invoking the privilege
  - Privilege protects only the communication, not the facts

COZEN O'CONNOR

# Attorney-Client Privilege


- While virtually all client confidences and communication with lawyers are “confidential” within the meaning of Rule 1.6, not all client communications with lawyers are privileged.
- Therefore, privilege applies only to certain communications with clients that meet the elements of privilege.
- In other words, what is “confidential” may not be protected by the privilege, but what is privileged is always confidential in nature.

COZEN O’CONNOR

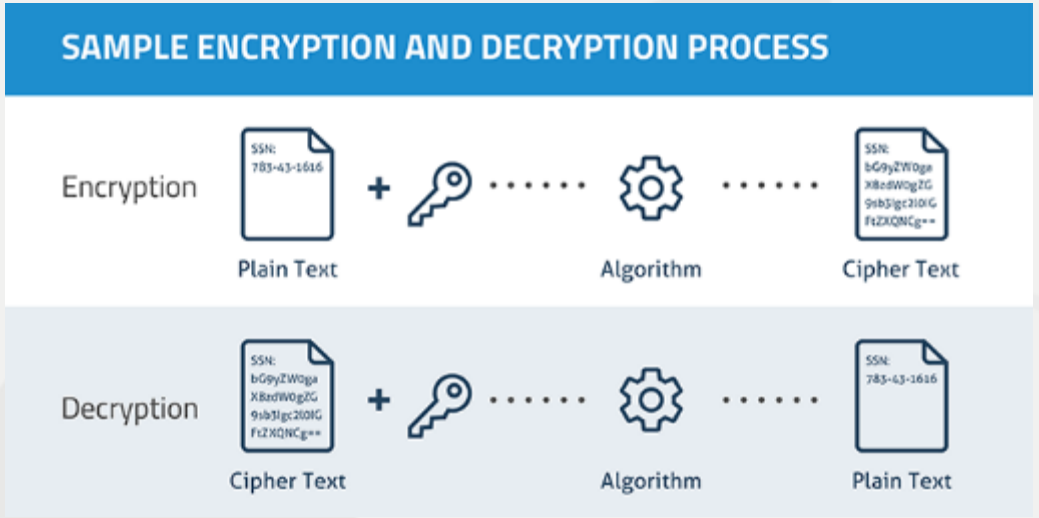
# When Confidential Information Becomes "Public"

- Just as a voluntary disclosure will result in waiver of the privilege, client confidentiality can be waived for information that has become "publicly known."
- Example – email
- Client forwards legal advice to third party
- Inadvertent reply all that includes legal advice
- Perils of email to opposing counsel with bcc to client
- Data breaches

COZEN O'CONNOR

# Encryption

- Encrypted personal identification numbers (PINs)
- Algorithm scrambled passwords (“hashed passwords”)




COZEN O'CONNOR

# Employee Training

- Comprehensive training for personnel, including attorneys, IT professionals, and staff.
- “63 percent of confirmed data breaches took place because of the use of weak, default, or stolen passwords.”
- Written policies managing information security expectations. Regulation of:
  - Passwords
  - E-mail
  - Digital data
  - Cloud computing
  - Social media
  - Non-work-related browsing
  - Use of personal devices

COZEN O’CONNOR

# Cloud Computing

- Exercise reasonable care to ensure materials stored in the cloud remain confidential.
- Employ reasonable safeguards to protect data from breach, data loss, and other risk.
- Provide reasonable supervision of cloud vendor.
- Discuss appropriateness of cloud storage with client if data is especially sensitive (e.g., trade secrets).
- Instruct the vendor to preserve the confidentiality of information.
- Conduct a due diligence investigation of any potential provider.
- Stay abreast of changes in technology.
- Review providers' security procedures periodically.

COZEN O'CONNOR

# Cyber Liability Insurance

- Many courts are holding that commercial general liability insurance policies do not cover cyber attacks.
- Can help mitigate the impact of data security failure, but can also include “pre-breach services” such as breach coaches, cyber-readiness analyses, and security awareness programs.
- Court interpretations of cyber insurance coverage have also narrowly construed the scope of the policies.

COZEN O'CONNOR

# Contact Information

David J. Walton

Cozen O’Connor

dwalton@cozen.com

COZEN O'CONNOR