PBI's Cyber Security, Ransomware, and Digital Ethics Webinar
June 10, 2020

More Than 100 Law Firms Have Reported Data Breaches. And the Problem Is Getting Worse
A Law.com investigation finds that law firms are falling victim to data breaches at an alarming rate, exposing sensitive client and attorney information. These incidents—most unpublicized before now—may just be the tip of the iceberg.
By Christine Simmons, Xiumei Deng and Ben Hancek | October 15, 2019 at 01:10 PM

How Vendor Data Breaches Are Putting Law Firms at Risk
Records show that law firms’ relationships with third-party vendors are a frequent point of exposure to cyber breaches and accidental leaks.
By Christine Simmons, Xiumei Deng and Ben Hancek | October 17, 2019 at 06:45 PM

Ethics Forum: Questions and Answers on Professional Responsibility
I saw articles about law firms being hacked with their data breached through hackers or unlawful/unauthorized users. What does that mean for the legal profession?
By Samuel C. Streiff | October 24, 2019
Terminology

**Protected Information** includes:
- **Confidential Client Information** and
- **Personally Identifiable Information** of individuals (or “PII”)

**PII** = Personal Identifiable Information, often identified in a statute, generally means information capable of identifying or contacting a person

**CCI** = Confidential Client Information includes any information relating to a lawyer’s representation of a client.
External Threat Events

- Phishing
  - Credential Theft
  - Malicious content
- Malware
  - Viruses
  - Worms
  - Ransomware
- Exploitable Vulnerabilities

80%
MALWARE INFECTIONS FROM EMAIL

Internal Threat Events

- Miscreant Insiders
- Negligence & employee error
- Improper disposal, over-retention
- Lost and stolen devices
- Shadow technology
- Misdirected communications
- Misconfigurations
- Negligence & employee error

28%
BREACHES INVOLVING INTERNAL ACTORS
Non-Cyber Threats:

- Improper handling of paper and other media containing sensitive data
- Private conversations in public places

Sources of Obligations

- Rules of Professional Conduct
- Contracts
- Court rules
- Statutes
- Practical considerations
Pa Rules of Prof’l Conduct

• Rule 1.1 - Competency
• Rule 1.6 - Confidentiality
• Rule 1.15 - Duty to safeguard client property
• Rule 5 - Duties to supervise
• Rule 1.9 - Duties to former clients

Rule 1.1 - Competency

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

• Cmt. 8: “[A] lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology”. 
Rule 1.6 - Confidentiality

• 1.6(a): “A lawyer shall not reveal information relating to representation of a client unless the client gives informed consent”.

• 1.6(d): “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.”

• Cmt. 25: “[A] lawyer should act in accordance with court policies governing disclosure of sensitive or confidential information, including the Case Records Public Access Policy of the Unified Judicial System of Pennsylvania. . . . 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 (d) if the lawyer has made reasonable efforts to prevent the access or disclosure.”

Rule 1.6 - Confidentiality

• Cmt. 25: Factors for reasonableness:
  • Sensitivity of info
  • Likelihood of disclosure if no add’l safeguards used
  • Cost and difficulty in implementing safeguards
  • Extent to which safeguards adversely affect lawyer’s ability to represent clients
  • Client may require special security measures or give informed consent to forego security measures
  • Rule does not address other legal obligations
Rule 1.6 - Confidentiality

• Cmt. 25: “[A] lawyer should act in accordance with court policies governing disclosure of sensitive or confidential information, including the Case Records Public Access Policy of the Unified Judicial System of Pennsylvania. . . . 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 (d) if the lawyer has made reasonable efforts to prevent the access or disclosure.”

Rule 1.6 - Confidentiality

• Cmt. 26: when communicating info relating to a client representation, lawyer “must take reasonable precautions to prevent the information from coming into the hands of unintended recipients.”

  • Use method with reasonable expectation of privacy

  • Circumstances may require special precautions
Rule 1.9 – Former Client Duties

• 1.9(c)(2): “A lawyer who has formerly represented a client . . . shall not thereafter . . . reveal information relating to the representation except as these Rules would permit or require with respect to a client.”

• See also 1.6(e): “The duty not to reveal information relating to representation of a client continues after the client-lawyer relationship has terminated.”

Rule 1.15 – Safekeeping Property

“A lawyer shall hold Rule 1.15 Funds and property separate from the lawyer’s own property. Such property shall be identified and appropriately safeguarded”.

Several state ethics decisions make clear that client files, including data provided by clients to their lawyer, are encompassed in the definition of “client property”.
Rule 5 – Duty to Supervise

5.1(b): “A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.”

5.3(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.”

• law firm staff, but also vendors

Other Ethical Obligations:

• ABA Formal Opinion 477 (2017)
• PBA Formal Opinion 2020-300
Contract Sources:

- Engagement Agreement
- Outside counsel standards
- Client Data Security Questionnaires
- Protective Orders
- Key provisions:
  - Access limits
  - Retention
  - Destruction/return/backup copies

Court Rules:

- Case Records Public Access Policy of the Unified Judicial System of Pennsylvania
- May require privacy for specified information:
  - Minor children names
  - Social Security numbers
  - Medical information
  - Other personal information
- Sealing and redacting
Other Legal Obligations:

• *Dittman v. UPMC*, No. 43 WAP 2017 (Pa. Nov. 21, 2018) – hackers stole data on 62,000 current and former UPMC employees. Lower courts found in UPMC’s favor.

• Pa. Supreme Ct.: “An employer has a legal duty to exercise reasonable care to safeguard its employees’ sensitive personal information stored by the employer on an internet-accessible computer system.”

Case Studies:

In our real-world examples:

• What could counsel have done better in those cases?

• What facts stand out as red flags?

• What policies or procedures would have helped to avoid the incident?
Case Studies:

• DLA Piper targeted by Petya malware

Case Studies:

• Panama Papers – 2016 leak of 11.5m files from fourth largest offshore law firm
Case Studies:


In Novel Case, Insurer Sues Own Law Firm After Data Breach

Case Studies:

Shore v. Johnson & Bell, LTD, No. 1:16-cv-04363 (N.D. Ill. Apr. 15, 2016): Edelson PC alleges in putative class action that Johnson & Bell, a mid-size Chicago-based law firm, was negligent and engaged in malpractice by allowing information security vulnerabilities to develop that created risks to client information.
Case Studies:

Millard v Doran, No. 2016-153262 (N.Y. Supr. Apr. 18, 2016) - complaint against lawyer for malpractice and breach of fiduciary duty for failure to protect client fund, integrity of client files, and confidentiality of communications.

Case Studies:

Reisinger v. Tri-County Abstract Servs., No. 2018-11186, 68 Cumb. 108 (2019) – court granted demurrer for unfair trade practices claim where both plaintiffs and escrow agent were defrauded in transfer of real estate sale funds.
Case Studies:

Leventhal v. MandMarblestone Group., No. 18-2727 (E.D. Pa. 2020) – dispute between law firm and the administrator of the firm’s retirement fund in which administrator argued that cyber-fraud theft from fund resulted from firm’s carelessness regarding data security and remote work.

Case Studies:

Hacker (as Bragg): Hi Mel (Staffin) - Are you going to be in the office tomorrow? I have wire [sic] for $380,000 to send to Midtown Resources for an Eagle Funding loan to them but this is going to Midtown Resources [sic] investment account in Hong Kong. Let me know so I [sic] can forward the wiring instructions to you first [sic] tomorrow, as tomorrow will be an [sic] busy day for me. Thanks . . .

Staffin: I am in tomorrow

Hacker: Mel - I just received Midtown Resources [sic] investment wiring instructions in Hong Kong see below.

* Bank Name: Bank of China Hk Ltd
* Bank Address: 774 Nathan Road Hong Kong
* Swift: BKCHHKHH
* Account Name: Cohen International Ltd
* Account #: 012-692-08409-8.
* Reference: Midtown Resources Eagle Funding

Please [*5] transfer from our trust account; they need a swift copy once the wire is sent, email that to me once you take care of this.

Thanks in advance . . .

At the time of these emails, Bragg was in Seattle, Washington. Staffin thus believed that Eagle Funding required a transfer in a time-sensitive manner and that Bragg was unable to execute the transfer while travelling on the west coast. Staffin was further convinced of the emails’ authenticity based on the hacker’s familiarity with the Eagle Funding representation and the IOLTA subaccount number, along with the use of Staffin’s nickname, Mel.

Later on December 7, the hacker, again posing as Bragg, contacted Staffin in attempt to secure another wire transfer of $980,000 from the Eagle Funding account to the Bank of China. After Staffin offered to call to discuss the request, the hacker broke off further communications.

What is alleged to have happened to the law firm here is indeed unfortunate. The computer hacker, of course, is the real culprit but is not a party to this lawsuit. For the reasons stated above, as between the law firm and the bank, the law firm must bear the loss based on the facts set forth in the amended complaint. Accordingly, the motion of Bank of America to dismiss the amended complaint will be granted.
Case Studies:

*Dentons Canada LLP v. Trisura Guarantee Ins. Co., (Ontario Superior Court Dec. 11, 2018)* – law firm sought insurance coverage after computer fraud duped associate into transferring $2.5 million to the wrong account for a real property sale.