5 Practice Tips for Law Firms as Data Breach Spotlight Swings Their Way

By Joseph J. Lazzarotti, Jason C. Gavejian and Damon W. Silver

June 9, 2016

While data breach incidents affecting the entertainment, retail, healthcare, and financial industries have garnered more attention in past years, the data breach spotlight recently shifted to law firms.

This shift was triggered by media coverage of the breach and leak of the Panama Papers, and by reports that, in 2015, hackers breached the networks of two well-known and highly-regarded U.S.-based firms, Cravath, Swaine & Moore and Weil, Gotshal & Manges. It also has been reported that a Russian cybercriminal recently attempted to breach the systems of dozens of other major firms, seeking insider information on which to trade.

Law firms, which tend to lag behind businesses in other industries in data security preparedness, are entrusted with financial, intellectual property, medical, and embarrassing personal data that may draw cybercriminals. Breaches of this data expose law firms to potentially massive liability. Erosion of client confidence and reputational injury may be the most obvious (and hardest to quantify) examples, but firms also are exposed to malpractice lawsuits alleging negligent handling of confidential client data and to state agency and private actions for failure, in the wake of breaches, to timely notify affected individuals, including employees, clients, and other parties and witnesses to litigations. Attorneys employed by firms that experience breaches also may be found to have violated the rules of professional conduct.

In light of these risks, law firms should act expediently to safeguard the data under their care. The following recommendations are non-exhaustive, but represent key actions law firms can take to prevent breaches from occurring and to effectively respond to them if they do.

1. Conduct a risk assessment and develop a comprehensive written information security program ("WISP"). Firms should start by establishing a team – made up of attorneys and employees from their HR, IT/IS, finance, government relations, marketing, or PR departments – to coordinate the risk assessment project. They should also select a project leader and secure upfront project approval from senior management. Firms should then inventory:

- what confidential data they maintain (different types of data – *e.g.,* medical and financial data – trigger different legal requirements);
- to whom that data pertains and where they reside (data security and breach response obligations vary based on the state and international laws implicated);
- where that data is stored (*e.g.,* on desktops, laptops, mobile devices, flash drives, and digital copiers);
- which employees and outside vendors have access to the data, and how it flows through the firm; and
- what safeguards are in place to protect data and detect breaches.

Not only are risk assessments critical to a law firm's breach prevention and response efforts, but failure to conduct them may expose it to penalties and other liabilities under federal and state laws.

After completing its risk assessment, a firm should develop a WISP designed to protect its data assets against breaches and to ensure that, if a breach occurs, the firm is prepared to respond effectively. A firm's WISP should address, at minimum:

- which individuals are responsible for ensuring compliance with federal and state data security and breach laws;
- data encryption, transport, monitoring, and destruction;
- employee and third-party access rights;
- email protocols (*e.g.,* how to detect and prevent email phishing attacks, which have become increasingly common and costly);
- remote access to the firm's system and storage of confidential data on mobile devices; and
- proper redaction of personal information in documents filed electronically.

Meet the Authors

Joseph J. Lazzarotti

Principal
Berkeley Heights 908-795-5205
Email

Jason C. Gavejian

Principal
Berkeley Heights 908-795-5139
Email

Damon W. Silver

Principal
New York Metro
New York City 212-545-4063
Email

Practices

Privacy, Data and Cybersecurity

Industries

Professional Services

Firms with small IT departments, or none at all, are not relieved of their data security obligations. The ABA Cybersecurity Handbooks cautions, "If a lawyer is not competent to decide whether use of a particular technology (*e.g.,* cloud storage, public Wi-Fi) allows reasonable measures to protect client confidentiality, the ethics rules require that the lawyer must get help, even if that means hiring an expert information technology consultant to advise the lawyer." Ethics opinions from numerous states likewise indicate that attorneys have affirmative obligations to learn what data security measures are required of them and to ensure that those measures are implemented.

2. Actively manage relationships with vendors. When engaging vendors (such as for e-discovery, accounting or computer forensics, or document destruction), firms should conduct thorough due diligence and include in their vendor contracts provisions regarding compliance with data privacy and breach laws. This due diligence should include vetting vendors to assess their industry reputation, financial condition, insurance coverage, and the adequacy of the data security training they provide their employees.

3. Include data security protections in telecommuting policies. In contrast to attorneys and staff working in the controlled environment of firm offices, telecommuters may access and transfer confidential and proprietary data from devices and over networks that lack adequate security protections. Firms should therefore: (a) evaluate the equipment and internet service providers their telecommuting employees use; (b) secure transmissions of data by these employees through the use of, for example, a virtual private network (VPN) or Citrix; (c) train employees on firm expectations regarding the off-premises handling of confidential data; and (d) monitor transmissions of data by telecommuters to evaluate compliance with relevant policies.

4. Scrub metadata. Firms frequently send "external" drafts of documents to outside parties, such as opposing counsel, which, prior to transmission, have been revised by the firms' attorneys and clients. Prior "internal" drafts of those documents (*i.e.,* drafts that were never intended to be seen by outside parties) likely contained confidential data, such as redlined comments or revisions revealing strategic or privileged communications, that the external drafts, on their face, no longer contain. Unless affirmative steps are taken to remove metadata (*i.e.,* data about data) from external drafts, however, the confidential information contained in prior internal drafts may be recoverable by recipients of the external drafts (or by hackers), resulting in potential data breaches and violations of the rules of professional conduct.

5. Obtain adequate insurance coverage. Standard professional liability insurance policies may cover breach-related damages sought by a client alleging that its firm negligently handled its confidential data. However, such policies may not cover, among other things, fees expended investigating a breach, including for computer forensic experts and other breach support vendors; costs associated with preparing and distributing breach notices; productivity lost when employees are diverted to breach investigation and response activities; and fees paid to public relations experts or to outside counsel.

Understandably, some law firms will balk at the upfront and continuing costs of breach prevention measures. However, given the increased likelihood that firms will experience breaches, and the devastating liability they may face if they do, prudent firms will view data security programs as worthwhile investments.

***

Jackson Lewis attorneys are experienced in advising clients on preventing and responding to data breaches. Please contact us with any questions.