ZYWAVE | Front Page News Professional Edition

Zywave Professional Front Page News - Friday, April 18, 2025

E-mail This Story Print This Story

How law firms and their clients can mitigate the risk and potential legal exposures of an adverse cyber Incident

By Richard J. Bortnick, Wilson Elser Moskowitz Edelman & Dicker

Like other professionals, lawyers often have access to clients' sensitive personal, healthcare, commercial, and operational data. In certain circumstances, lawyers may have access to an individual's Protected Health Information (PHI) and/or Personally Identifiable Information (PII) such as financial information, drivers' license numbers, Social Security numbers, and the like (collectively, PHI/PII). At the same time, law firms may possess trade secrets, intellectual property, merger and acquisition details, and confidential attorney-client privileged data relating to their business clients. As a result, lawyers, like their clients, face the risk of a cyber event that can adversely affect a client's financial and/or medical positions as well as a commercial client's profits, reputations, functionality and, perhaps, continuing economic viability.

An important way for lawyers (and other professionals) and their clients to manage the risks attendant to the electronic storage of data and the ability of users to remotely access a law firm's or client's data storage facilities is for them to take reasonable steps to create and implement cyber, privacy, and technology (CPT) protocols before something goes wrong. This should include the purchase of dedicated CPT-specific

insurance. At the same time, in the case of an individual's PHI/PII, federal and state laws and regulations require law firms and others holding such data to take all reasonable steps to protect it. In turn, contracts with business clients also may contain such mandates.

So too, ABA Model Rule 1.6, *Confidentiality of Information*, dictates that lawyers should "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Insofar this is a Model Rule, it is not binding unto itself on attorneys. Still, each state and territory has its own ethical rules which may adopt this Model Rule or a similar dictate.

To comply with their ethical and regulatory obligations, a law firm must make reasonable efforts to protect its clients' data. This could mean implementing a data security policy as well as business continuity and incident response plans, employee training, use of strong passwords and required password changes every three to six months, encryption, multifactor authentication, securing mobile devices, improving communication practices through email, off-network backups, and vetting legal tech providers. It also implicates policies and procedures governing employees' unapproved applications, tools and personal devices which do not go through security testing, leaving the firm vulnerable to malware, phishing and ransomware attacks.

Risks of a CPT event

Business entities, regardless of whether they employ outside legal counsel, must be sensitive to the widespread impact of an adverse CPT event, such as a breach or employee negligence starting with loss of customer goodwill and reputational damage. Both clients and their outside counsel holding sensitive information are at risk of impacts to such confidential data as the result of an antagonistic cyber event, such as a hacker intrusion, ransomware, the unintentional loss of tangible property containing PHI/PII or sensitive corporate information (such as lost laptops and hard drives), and business email compromises (BEC). It doesn't matter whether the harm is attributable to malicious activity or simple employee or third-party error. It's the effect of the loss of sensitive or protected data that counts, and in many cases the effect of a cyber event can be devastating, if not fatal, to the economic viability and vitality of a business and a law firm as well as an individual client's financial and healthcare positions.

According to the American Bar Association's 2023 *Legal Technology Survey Report,* close to 30% of law firms nationwide reported having experienced a data security

incident. Moreover, IBM's *2024 Cost of a Data Breach Report* estimates the average cost of a global data breach affecting professional organizations to be in excess of $5 million. And the theft and/or loss of data has continued into 2025. Indeed, just recently, two law firms were sued by a client when an attorney erroneously wired more than $400,000 in client funds to a cybercriminal as a result of a BEC wherein the fraudster allegedly used spoofed email accounts to trick the attorney into wiring the funds to the scammer's bank account. And, regrettably, it seems as though something like this happens every day along with, in many cases, resulting in cyber class action lawsuits where multiple individuals' PHI/PII are accessed or acquired by a threat actor.

As lawyers, we regularly advise our clients to implement and employ best practices when consulting on commercial, risk management, and loss avoidance strategies. However, many outside (and sometimes in-house) counsel continue to use outdated cybersecurity programs and are not regularly trained and updated on CPT best practices, potentially exposing the lawyers (and their clients) to a potential cyber event impacting their information.

In the case of a cyber event, as in other contexts, both clients and their outside attorneys should look to specialized legal counsel and IT specialists to create, implement, and regularly update a best practices regime. The advantage of engaging an attorney, with the attendant attorney-client privilege, is manifest. As in many other situations, when employees, outside counsel, and others are being educated on CPT best practices, the privilege can be a critical asset. Hence, while vendors and IT specialists (both internal and external) may promote themselves as having the appropriate knowledge and training to teach and implement CPT best practices, they do not possess the protections afforded by the attorney-client relationship. In the rapidly evolving area of CPT, the privilege becomes even more important, as many companies' management, employees, and outside advisers who face CPT risks on a daily basis are just at the start of the learning curve.

Why law firms and their clients should be concerned

Many individuals and business clients fail to consider the fact that their outside counsel likely hold both their own sensitive data and that of third parties – that is, a company's clients or customers. For example, outside counsel might control and/or have access to PHI/PII and confidential corporate information such as trade secrets. To put it another way, outside counsel could hold the keys to the kingdom, and that means they could lose them.

The list of what can constitute PHI/PII is long. It can, for example, consist of a person's last name together with their address, telephone number, electronic mail address, biometric information, photographs or computerized images, a password, an official state- or government-issued driver's license or identification card number, a government passport number, an employer or student identification number, a military identification number, date of birth, medical information, financial information, tax information, disability information, and zip codes. At the same time, a law firm likely will hold information about a commercial client's intellectual property, financial information, and other highly sensitive data that in the wrong hands can devastate a business.

Virtually every law firm holds at least one or more of these categories of information about their clients. Firms should therefore engage privacy counsel to understand the potential regulatory regimes applicable to that information. Could the health records in a lawyer's custody not only be subject to state law but also be protected under HIPAA?

It is common knowledge that personal health information is governed by HIPAA and HITECH. Both laws apply to "covered entities," i.e., healthcare clearinghouses, health plans, and healthcare providers that conduct certain functions in electronic form.

What is less well known is that HIPAA and HITECH also apply to "business associates" that provide services involving the use or disclosure of personal health information held on behalf of a covered entity. Such business associates typically create, receive, maintain, or transmit personal health information on behalf of their covered entity clients. For example, a business associate can include vendors that provide billing- and collection-related services, file maintenance, etc. Critically, a lawyer can also be a "business associate" subject to certain HIPAA requirements.

Lawyers should evaluate whether their firms fall within HITECH's definition of "business associate" to the extent they provide "services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected individually identifiable health information …." In the event a law firm obtains PHI in order to provide professional services to a "covered entity" such as a hospital or health care provider, "business associate'" status may attach, regardless of whether or not the law firm has signed a "business associate" agreement with its "covered entity" client, as required under HIPAA. Commentary to HITECH adds a fine point, stating that "a person becomes a

business associate by definition, not by the act of contracting with a covered entity or otherwise. Therefore, liability for impermissible uses and disclosures attaches immediately when a person creates, receives, maintains, or transmits protected health information on behalf of a covered entity or business associate and otherwise meets the definition of a business associate."

But HIPAA and HITECH do not stand alone in the federal regime. Other federal agencies mandating the use of enumerated safeguards include the Federal Trade Commission and the Securities and Exchange Commission. Equally problematic, a growing number of states are enacting laws that require companies holding an individual's PHI/PII to employ mandated security procedures lest the company be subject to an Enforcement Action and severe fines and penalties. A law firm and its clients should identify and comport with such local state rules to ensure they are in compliance, And, again, there is always the looming threat of a putative class action brought by individuals affected by a cyber-related event. The costs attendant to such matters are only increasing, sometimes exponentially, and almost certainly into the millions, if not tens of millions, of dollars.

In short, there are real and material risks attendant to a company's or law firm's failure to comply with governing cybersecurity laws and regulations.

Cyber-specific insurance

As independent counsel, we are required by state law to purchase errors and omissions insurance. Regrettably, law firms (and their clients) assume that the law firm's E&O and CGL policies will cover CPT risks. This is a critical mistake. Indeed, more than a few insurance brokers and policyholders misunderstand the extent and limitations of E&O and CGL insurance.

In particular, many mistakenly believe that advertising and personal injury coverage (typically Part B or Part II of a CGL policy) covers a cyber breach. Others are of the view that an E&O policy will respond. In a majority of situations, these views are wrong.

Although limited CPT-related insurance may be provided by a CGL or E&O insurance policy or an Endorsement covering third-party risks, the lion's share of fees, expenses, and other loss incurred following a CPT incident would not be covered, CGL policies cover damage to a third party's tangible property (or person) as well as, in certain situations, advertising and personal injury (if purchased). In turn, E&O forms apply to professional negligence. These types of insurance coverages typically do not cover incident response costs such as the fees and expenses of legal counsel, IT

forensic investigators, data mining vendors, data restoration companies, and notification/ credit monitoring providers, which generally make up the largest financial outlay following an adverse cyber-related incident. Moreover, if information from either an open or closed matter still rests on a law firm's server and such information is malicious accessed or negligently lost and the law firm is subsequently sued by a client or other third party whose sensitive information has been accessed or acquired, or even simply lost by an employee, it could be difficult for firm to credibly argue that the mere storage of such information constitutes a "professional service", which generally encompasses the delivery of specialized expertise and advice to clients, often focusing on specific areas of business or technology. Courts have not yet adjudicated this issue, although the argument is often raised by insurers facing such situations.

The same precept may apply to a law firm's vendors, such as a managed service provider or data storage company that has access to a law firm's sensitive data and which may be the entity responsible for enabling or causing an adverse cyber event. In any event, neither a CGL nor an E&O policy typically applies to either first-party loss or crisis management expenses, although a law firm and its clients should study and speak with their broker about whether such insurance is being provided, and, if not, if they can purchase an endorsement covering such expenses, recognizing that any associated limits of liability likely will be relatively modest, perhaps in the range of $100,000 or less (sometimes, $25,000).

In stark contrast, CPT insurance can cover a law firm's (and, by extension, perhaps a client's) crisis management–related costs and expenses. Because of this, we regularly advise clients (almost on a daily basis) to require their vendors (including outside counsel) to purchase dedicated CPT insurance. At a minimum, this would be an incentive, if not a mandate, for counsel's adoption of best practices, which if handled correctly will reduce the risk of an adverse CPT incident. Of equal value, outside counsel's deployment of a best practices regime often can help reduce the premium a law firm pays for CPT insurance.

Conclusion

In short, CPT insurance is a unicorn unlike any other. Companies and law firms purchase property insurance to protect them against fires, earthquakes, and other natural disasters. Why, then, would they not purchase CPT insurance, which is designed to cover an insured's most valuable assets, the theft of which could either bankrupt a firm or, at least, severely damage their reputations? CPT attorneys ponder this question every day. Shouldn't you?

Richard Bortnick is Of Counsel in law firm Wilson Elser's Cybersecurity & Data Privacy practice. He is an industry-renowned problem solver who litigates and counsels U.S. and international insurers and corporations on cyber, privacy and technology risks and exposures; directors & officers liability; insurance coverage; products liability; and commercial litigation matters. Richard was named Advisen's Cyber Risk Champion of the Year in 2015.