Cyber Incidents Create a Variety of Ethical Obligations

If you haven't yet been the victim of a cyber breach or other cyber incident, you will be. When that happens, what should you do? How do you handle all the competing obligations to your clients, the Bar, and related third parties?

The New York City Bar recently published Formal Opinion 2024-3, Ethical Obligations Relating to a Cybersecurity Incident, which addresses many of the questions that arise in this situation. Because it's a relatively recent opinion (July 2024), it encompasses much of the advice and direction that have been provided over the years by other bar associations addressing the same subject. Note, however, that because certain jurisdictions may have specific rules or requirements, you should check for opinions and guidance in your state of licensure before taking action or creating a plan to respond to a cyber incident.

In short, the NYCB opinion provides the following guidance:

- Lawyers and law firms have an obligation of technological competence under Rules 1.1, 1.3 and 1.6 to take appropriate steps to protect clients' confidential data.

- In the wake of a cybersecurity incident, lawyers and law firms may have statutory, regulatory, or contractual obligations to notify clients and other third parties. Separate from and in addition to those obligations, lawyers and law firms have an ethical obligation under Rule 1.4 to promptly notify current clients when a cybersecurity incident occurs that constitutes a "material development" in a representation or must be explained to the client to permit the client to make an informed decision regarding the representation. Although Rule 1.4 does not require notification to former or prospective clients, lawyers may decide, where reasonable, to notify former or prospective clients who are likely to have been harmed as a result of the loss or theft of their sensitive confidential information in a lawyer's or law firm's cybersecurity incident.

- If a lawyer or law firm chooses to negotiate with the cyber-extortionists in order to regain system access or protect client information, generally accepted conventions, as well as the underlying rationale of Rules 4.1 and 8.4(c), public policy and the societal good, permit being not candid to those cyber-extortionists about facts relating to the impact of the cyber attack, the victim's financial situation, and any actions taken to mitigate the damage caused by the attack.

- While not a common occurrence, in situations where a lawyer or law firm receives advance notice of an impending cybersecurity attack through a threat by the cyber-extortionist, a lawyer or law firm must take reasonable efforts to determine the nature of the threat and what, if any, actions the lawyer or law firm can take to prevent or ameliorate any effects to client information or to the lawyer's ability to competently and diligently represent clients. Rule 1.4 does not require current clients be notified of the cyber threat; however, if the lawyer or law firm reasonably believes that it may have to push back important meetings or events (g., an imminent deal closing, start of trial, or a deposition) for certain client matters because of the likely effects of a credible cyber threat on its ability to perform the necessary work, the lawyer or law firm should promptly inform the affected clients that emergent circumstances have arisen and advise them of the efforts that the firm is taking to reschedule those meetings or events.

- When a lawyer or law firm is the victim of a cybersecurity incident, there is no ethical prohibition against paying, or obligation to pay, a ransom.

- Rule 1.7 may prohibit lawyers or law firms from continuing to represent (or from taking on a new representation of) a client whose confidential information has or may be compromised in a cybersecurity incident if (1) the client's obligations to or interest in further reporting the cybersecurity interest differ from the lawyer's or law firm's interests; or (2) the client may have a claim or has expressed that it may have a claim of malpractice or breach of fiduciary duty against the lawyer or law firm as a result of the cybersecurity incident.

- A lawyer or law firm that is the victim of a cybersecurity incident and wishes to report it to law enforcement or cooperate in a governmental investigation into the incident must be cognizant of its continuing confidentiality obligations to current, former, or prospective clients under Rules 1.6, 1.9 and 1.18, and of the potential adverse effects to the clients that may result by reporting information to the government. In making a disclosure to the government, the lawyer should consider whether it should: (1) report the incident but not disclose the clients whose files were taken or other confidential client information; or (2) obtain consent from the affected clients, former clients or prospective clients to the disclosure of client confidences to the government; or (3) limit disclosures to those client confidences that are reasonable and impliedly authorized to advance the best interests of the clients, such as by stopping an ongoing breach or recovering a clients' confidential information.

For further or more specific guidance on this topic, don't hesitate to get in touch with our senior risk management attorneys. To obtain a consultation, you should log in to Attorneys Risk Management, and click on the "Request a Risk Management Consultation" button.