|  |  |  |  |
| --- | --- | --- | --- |
| **ABA Formal Opinion 477R: Securing communication of protected client information** June 2017 | Eye on Ethics |  |  | **Best Practices for Victim Response and Reporting of Cyber Incidents**Version 1.0 (April 2015) |
|  |   |  |  |
|  |   |  |  |
| The committee recommended the following steps lawyers should take to guard against disclosures, including: |   |  |  |
|  |   |  |  |
| **1. Understand the nature of the threat.**Consider the sensitivity of the client’s information and whether it poses a greater risk of cyber theft. If there is a higher risk, greater protections may be warranted. |  |  |   |
|  |  |  |  |
| **2. Understand how client confidential information is transmitted and where it is stored.**Have a basic understanding of how your firm manages and accesses client data. Be aware of the multiple devices such as smartphones, laptops and tablets that are used to access client data, as each device is an access point and should be evaluated for security compliance. |  |  |   |
|  |  |  |  |
| **3. Understand and use reasonable electronic security measures.**Have an understanding of the security measures that are available to provide reasonable protections for client data.  What is reasonable may depend on the facts of each case, and may include security procedures such as using secure Wi-Fi, firewalls and anti-spyware/anti-virus software and encryption.    |  |  | Organizations should have a plan in place for handling computer intrusions before an intrusion occurs. During an intrusion, an organization’s management and personnel should be focused on containing the intrusion, mitigating the harm, and collecting and preserving vital information that will help them assess the nature and scope of the damage and the potential source of the threat. A cyber incident is not the time to be creating emergency procedures or considering for the first time how best to respond.The plan should be “actionable.” It should provide specific, concrete procedures to follow in the event of a cyber incident. At a minimum, the procedures should address:• Who has lead responsibility for different elements of an organization’s cyber incident response, from decisions about public communications, to information technology access, to implementation of security measures, to resolving legal questions; |
| **4. Determine how electronic communications about clients’ matters should be protected.**Discuss with the client the level of security that is appropriate when communicating electronically. If the information is sensitive or warrants extra security, consider safeguards such as encryption or password protection for attachments. Take into account the client’s level of sophistication with electronic communications. If the client is unsophisticated or has limited access to appropriate technology protections, alternative nonelectronic communication may be warranted.    |  |  | • How to contact critical personnel at any time, day or night; • How to proceed if critical personnel is unreachable and who will serve as back-up; • What mission critical data, networks, or services should be prioritized for the greatest protection; • How to preserve data related to the intrusion in a forensically sound manner; • What criteria will be used to ascertain whether data owners, customers, or partner companies should be notified if their data or data affecting their networks is stolen; and • Procedures for notifying law enforcement and/or computer incident-reporting organization.Incident response plans may differ depending upon an organization’s size, structure, and nature of its business. Similarly, decision-making under a particular incident response plan may differ depending upon the nature of a cyber incident. In any event, institutionalized familiarity with the organization’s framework for addressing a cyber incident will expedite response time and save critical minutes during C2an incident. |
| **5. Label client confidential information.** Mark communications as privileged and confidential to put any unintended lawyer recipient on notice that the information is privileged and confidential. Once on notice, under Model Rule 4.4(b) Respect for Rights of Third Persons, the inadvertent recipient would be on notice to promptly notify the sender.  |   |   |   |
| **6. Train lawyers and nonlawyer assistants in technology and information security.**Under Model Rules 5.1 and 5.3, take steps to ensure that lawyers and support personnel in the firm understand how to use reasonably secure methods of communication with clients. Also, follow up with law firm personnel to ensure that security procedures are adhered to, and periodically reassess and update security procedures. |  |  | **F. Ensure Organization Policies Align with Your Cyber Incident Response Plan**Some preventative and preparatory measures related to incident planning may need to be implemented outside the context of preparing a cyber incident response plan. For instance, an organization should review its personnel and human resource policies to ensure they will reasonably minimize the risk of cyber incidents, including from “insider threats.” Proper personnel and information technology (IT) policies may help prevent a cyber incident in the first place. For instance, a practice of promptly revoking the network credentials of terminated employees—particularly system administrators and information technology staff—may prevent a subsequent cyber incident from occurring. Furthermore, reasonable access controls on networks may reduce the risk of harmful computer misuse. |
| **7. Conduct due diligence on vendors providing communication technology***.*Take steps to ensure that any outside vendor’s conduct comports with the professional obligations of the lawyer.  |  |  |   |
|  |  |  |  |
|  |  |  |  |