ANALYSIS

Attorney Cybersecurity Competence: Legal and Ethical Requirements Imposed by the SHIELD Act

An integral component of competency to practice law includes becoming educated—on a continuing basis—with both internal practice-focused as well as client-directed cybersecurity concerns.

October 07, 2022 at 10:00 AM

Cybersecurity

By Steven W. Teppler and Lauren X. Topelsohn | October 07, 2022 at 10:00 AM

A substantial portion of today's legal practice is conducted digitally and on-line. Attorneys generate, collect, store and use an abundance of client confidential information, personally identifiable information, protected health information, and information, the disclosure of which is either restricted or prohibited by statute or court order. Thus, the type of information that is part and parcel of the practice of law makes attorneys and law firms low hanging fruit for cybersecurity compromise.

Cybersecurity challenges for attorneys arise from remote work, using a variety of computing devices and methods (desktops, laptops, mobile devices) and "cloud" or "virtualized" computing, etc. that amplify an attorney's professional and ethical obligations directed to competency, confidentiality, and supervision.

N.Y. Gen. Bus. Law §899-bb, frequently referred to as the "New York SHIELD Act" includes cybersecurity requirements for businesses (including law firms) that own or license computerized private information of New York residents.

The Act requires that covered businesses maintain "reasonable safeguards to protect the security, confidentiality and integrity of the private information [of a New York Resident]" including, but not limited to, disposal of data." Section 899-BB (c)2.

Ascertaining *and maintaining* "reasonable" security is evaluated from on objective standard; in other words, what a reasonably prudent attorney would do under similar circumstances.

Moreover, effective Jan. 2, 2023, attorneys registered to practice in New York must complete at least one credit hour on cybersecurity, privacy and data protection as part of their biennial continuing legal education requirement. Joint Order amending 22 NYCRR 1500 Cybersecurity CLE requirement 06-10-22.

Law firms, regardless of size, must take appropriate measures to develop and maintain cybersecurity competency—and engage in a continuing program aimed at compliance, which is not possible without first assessing the risk of a cybersecurity incident.

It's All About Assessing Risk

The SHIELD Act mandates an understanding of risk assessments, which are necessary in order to obtain and maintain reasonable security. But this in turn requires an understanding of the risks attendant to practice law in the 21st Century.

What is 'Risk'? From a cybersecurity perspective, risk is defined as "[a]n effect of uncertainty on or within information and technology. Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and assets, individuals, or other organizations." (Definition based on ISO Guide 73 [6] and NIST SP 800-60 Vol. 1 Rev. 1 [7]) Source(s): NISTIR 8286 from ISO Guide 73 – Adapted, NIST SP 800-60 Vol. 1 Rev. 1 -; see https://csrc.nist.gov/glossary/term/cybersecurity_risk.

But compliance involves taking proactive measures in response to the risk assessment.

Acting on the Risk Assessment: There are four ways in which a law firm or lawyer can minimize cybersecurity risks.

Risk Avoidance: Simply avoid the activity that creates the risk. However, this is not practical. Lawyers share information, communicate with clients and adversaries, and in both the federal and most state court systems, are required to file almost all documents online. To avoid risk in this manner would be tantamount to giving up the practice of law.

Risk Mitigation: Risks can never be eliminated, but may be mitigated by implementing reasonable administrative, technical and physical safeguards described below to both minimize risk and mitigate the impact of a cybersecurity incident.

Risk Transference: Risks can be minimized in part by transferring the liability to a third party through cyber insurance or contract indemnification provisions with third parties. While this approach may limit monetary or financial liability, it does not address or prevent problems arising from regulatory proceedings or other non-monetary penalties. Moreover, cyber insurers are not only now taking a harder look at a potential insured's cybersecurity attestations before issuing coverage, they may seek to rescind an entire policy in the event a single attestation is misleading.

The New York SHIELD Act's three information-protective "safeguards" (aka "controls" or "compensating controls") can help law firms jump start their cybersecurity efforts. Those three safeguards or controls are administrative, technical and physical. Such safeguards should be implemented and maintained in a coordinated manner. In particular, administrative (managerial) and technical (IT) efforts should be coupled in order to mitigate security threats.

Shield Act Key Components: Risk Mitigation

Reasonable Administrative Safeguards. This component of the SHIELD Act focuses on the policies, procedures, and processes that should be implemented to support cybersecurity and include:

Cybersecurity Policy Development, Monitoring and Enforcement: This includes, to name a few, policies for cybersecurity backup, incident response, business continuity, disaster recovery, password management, patch management, change management, acceptable use, mobile device management, and third party/vendor management, Bring Your Own Device (BYOD), and remote work.

Security Program Coordination: Designate one or more trained individuals to coordinate and manage the security program. Components of a robust security program include:

• Identification of reasonably foreseeable internal and external risks. These could arise from intentional or unintended acts by firm staff (including partners and shareholders), as well as outside contractors.

• Assessing the sufficiency of safeguards in place to control the identified risks. This typically involves coordination between administrative and technical personnel.

• Training and managing employees security program practices and procedures. This requires both initial and periodic updates to address changes in personnel, firm structure, technology environment or other external.

• Selecting service providers capable of maintaining appropriate safeguards. This requires vetting and receiving adequate and expressly articulated cybersecurity assurances from firm service providers, and especially from those managed cloud service providers that store or processing a firm's sensitive, client confidential, or other information where unauthorized disclosure would trigger regulatory investigation or civil liability.

• Adjusting the security program in light of business changes or new circumstances. Such changes could render a system obsolete (and expose a vulnerability). Internal changes include system, software, and managed software providers. External events include managed service provider compromise; client or regulator mandated system upgrades or changes, etc.

Reasonable Technical Safeguards. These safeguards address a firm's information infrastructure and environment.

Assess risks in network and software design: Supervisory responsibilities don't stop at a firm's IT office doorstep. Attorney regulatory, professional and ethical obligations to assess and mitigate risk remain even if your information network is managed internally by employees or outsourced to third party managed service providers.

Assess risks in information processing, transmission and storage: Maintaining client confidences and other sensitive information (PHI, PII, etc.) means assessing and implementing solutions to protected information whether in transit, at rest (in storage) and in use. For example. various data protection technologies and techniques such as encryption and identity authentication are widely and commercially available at a variety of price points.

Detect, prevent and respond to attacks or system failures: Assess and implement firm- or practice-appropriate technical protections against data compromise and loss (e.g., prevention, intrusion detection, anti-virus, firewalls, and other malware protections).

Regularly test and monitor the effectiveness of key safeguards, systems and procedures: Testing of detective and preventive controls designed to mitigate risk should be conducted on a periodic basis.

Reasonable Physical Safeguards. Assess the risks attendant to information storage and disposal particularly confidential or sensitive information. This can also mean erasing electronic media so that the information cannot be read or reconstructed.

Law firms must become and remain competent and to achieve and maintain reasonable, defensible security in connection with protecting the confidentiality, integrity and availability of sensitive personal information whose unauthorized disclosure or impairment may lead to regulatory, disciplinary or civil liability. Developing practice-appropriate technical, administrative, and physical safeguards is legally required by New York's SHIELD Act. This in turn requires a corresponding understanding of risk, the performance of a risk assessment, and a proactive response to that assessment in a defensible, objectively reasonable manner.

Many non-legal enterprises have created either an in-house or retained Chief Legal/Cyber Officer position, which serves as the focal point for cybersecurity compliance, as well as incident detection, response and mitigation. In light of today's heightened legal and ethical obligations described above, law firms should consider designating a firm attorney (or outside counsel) who understands these legal and ethical obligations, who has the competence to act as Chief Legal-Cyber Officer, and who will be responsible for the firm's continuing efforts to achieve and maintain reasonable security.

Steven W. Teppler *is of counsel at Mandelbaum Barrett and chair of the firm's privacy and cybersecurity practice group.* **Lauren X. Topelsohn** *is a partner in the practice group. They may be reached at steppler@mblawfirm.com and ltopelsohn@mblawfirm.com, respectively.*