PRIORITIZING CYBERSECURITY

Lawyers today face enormous pressure in real time to adopt new technologies and those who do not may find it difficult to satisfy clients who expect immediate and continuous access to their attorney. The rules of professional conduct impose a duty on lawyers to provide competent representation, and the term "competence" would include at least a working familiarity with the technology that makes up much of the fabric of the clients' day-to-day lives from a personal and professional perspective.

The accelerated, wholesale adoption of new technologies has enabled law firms to benefit from web-based storage and transmission of vast amounts of highly confidential digital information. The real challenge; however, is motivating the lawyer to understand and mitigate the risks of adopting these technologies in the practice of law which makes the law firm vulnerable to cyberattack.

Balancing the duty of competence through enhanced technology with maintaining confidentiality is the real challenge for lawyers and law firms. Accomplishing this balance is a delicate manuever when cloud-computing services wield user agreements dense with exculpatory language and insistence that data security is never a one hundred percent guarantee. If the lawyer prioritizes cybersecurity in their practices, he or she will have the ability to address the inherent risks and satisfy the client demands.

The concept of "cybersecurity" stymies many lawyers, who assume it requires an in-depth grasp of a digital landscape which is wholly unfamiliar to most legal practitioners. Prioritizing cybersecurity requires the attorney to operate with a new mindset, one that requires them to consider the benefits and the costs of a new technology, with a sense of urgency on how to eliminate or at minimum, reduce, any of its risks, particularly the risk of cyberattack.

The mindset is paramount; however, there exists in the marketplace excellent tools to ensure that cybersecurity becomes, and remains, a priority—tools that enable attorneys to evaluate and diminish risk, while preparing for the unavoidable costs that come with using web-based services. We have outlined some simple steps to begin the process.

1. Invest in experts. Enlisting the support of data security experts is absolutely critical. Virus programs that can be downloaded off of the internet or a high-school intern who seems familiar with the Google Cloud platform are no substitutes. Importantly, however, obtaining expert help is only the first step. Experts alone cannot develop a firm culture that prioritizes cybersecurity, and having an expert on board may lure some lawyers into thinking that their firms are impervious to cyberattack. This is a dangerous misconception.

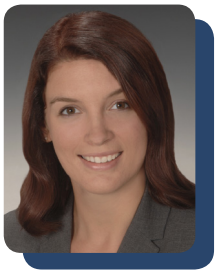
2. Consider cyber insurance. Former FBI director Robert Mueller infamously claimed in 2012 that "there are only two types of companies: those that have been hacked, and those that will be." Prepare for the worst, and consider some form of cyber insurance. Preventative measures are critical, but as nearly any cyber security expert will tell you, when it comes to data storage and transmission over the internet, there are no guarantees.

3. Implement a cybersecurity strategy. Insurance alone will not remedy all aspects of a serious data breach. If a cyberattack occurs, or client data is compromised, how will the firm respond? Who will the firm contact? Will outside counsel be hired? Develop a thorough strategy for response, and crucially, run tests to assess that response regularly.

4. Educate your team. The highest-quality cybersecurity measures can easily be defeated by an employee who unthinkingly uses the same password for all of his personal and professional accounts. Create a user-friendly data security policy, and provide consistent and frequent guidance on cybersecurity protocols. Rely on data security experts to assist in this effort.

5. Remain vigilant. Cybersecurity must become, and remain, a priority. Firms must continue to retain experts, train and retrain staff, develop response strategies to security breaches, and weigh the benefits and risks of adopting new technologies.

Lawyers face unique pressures to adopt new technologies while at the same time they must achieve client goals and expectations. Attorneys are privy to enormous amounts of confidential client data which make their data banks targets for hackers who have consistently viewed law firms as easy prey. This perception changes as lawyers are more diligent in securing the data and respecting the importance of cybersecurity.



Samantha Clarke

Associate

Samantha Clarke is an Associate with Pannone Lopes Devereaux & O'Gara LLC and a member of the Corporate & Business and Litigation Teams. She concentrates her practice on providing legal support, advocacy and counsel representing clients including performing pre-trial investigation and discovery, and motions and pleadings preparation through trial, settlement and the appeal process.

Gary R. Pannone

Managing Principal

Gary R. Pannone is the Managing Principal of Pannone Lopes Devereaux & O'Gara LLC. He has been representing closely held business owners for 30 years, specializing in the areas of business formations, corporate restructuring, mergers and acquisitions and corporate compliance. Attorney Pannone's practice also includes the representation of nonprofit organizations with respect to consolidations and mergers and acquisitions, and he serves on several boards and governance committees of nonprofit agencies. He is a frequent lecturer and published author in the areas of corporate compliance, board governance and best practices.

PANNONE LOPES DEVEREAUX & O'GARA LLC

counselors at law