Helping Lawyers Comply with Cybersecurity Rules

Introduction

In a previous article we raised the importance of helping our clients navigate the new world of cybersecurity. As lawyers, we can't forget that we need to navigate that world ourselves. Cybersecurity rules already apply to us and we already have duties under the law. Those duties come from our ethical obligations, from statutes and derivatively from rules binding upon our clients.

Horrifying security breaches fill the daily news, making 'cybersecurity' seem like an oxymoron. And in truth, we are learning that cyber data is exceedingly 'unsecure.' It is vulnerable to loss by human error and it is targeted for theft or destruction by a seemingly endless line of talented hackers, who are indeed continuing to focus upon law firms. It is not necessarily that our own work is of particular interest, rather that hackers realize we may have information from or about our clients that could be valuable. The client may have a very high level of security and we, as their lawyers, may be the weak link. In the cybersecurity literature, law firms are now viewed as very high value 'soft targets.'

For example, a New York City law firm was recently visited by the FBI. The Special Agent asked for a short meeting with the managing partner. The Agent reported that during a recent foreign criminal investigation the FBI had searched a server being used for criminal purposes. The agent explained that ALL of the firm's records were found on that foreign server.

Additionally, in a recent study by LogicForce involving a survey of 200 law firms, two thirds reported they had some sort of cyber breach, 53% did not have a response plan, and 100% were not compliant with their clients' cybersecurity policies.

It does appear that law firms will soon be on equal footing with mainstream businesses in needing to prevent and react to cybersecurity breaches. As our previous article urged, there are two critical components to this discussion; the legal framework and the technical measures. This article gives a brief overview of the legal framework that forms the cybersecurity duties placed upon lawyers and law firms.

There are three primary sources of cybersecurity duties that attorneys must comply with:

(1) Attorneys have ethical obligations regarding competent representation and confidentiality which now include cybersecurity requirements;

(2) Lawyers and their firms, in functioning as a business, can be directly subject to cybersecurity statutes relating to the handling of credit cards, employee health information, employee credit information, and other types of private data; and

(3) Lawyers can be derivatively subject to cybersecurity requirements imposed upon their clients.

Ethical Obligations on Lawyers

Longstanding ethical obligations have been amended to incorporate cybersecurity.

In 2012 the American Bar Association amended the Model Rules of Professional Conduct to explicitly impose, for the first time, cybersecurity obligations on attorneys. Washington State followed suit, amending the Washington State Rules of Professional Conduct to largely mirror the ABA's Model Rules. For purposes of this article they will be discussed together. The Rules now extend two principal ethical obligations to cybersecurity: competency and confidentiality.

First, a lawyer's duty of competency now includes technology. Comment 8 to Rule 1.1 was specially amended to reference technology and now states, "a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."

Second, a lawyer's duty of confidentiality extends to electronic documents and data, placing upon attorneys an affirmative duty to make a 'reasonable effort' to prevent the unauthorized access of client information. Comment 18 to Rule 1.6 indicates 'reasonableness' is a fact-based inquiry and while the ABA declined to require any specific security measures, the Comment does instruct that lawyers must have a 'process' to assess risks, and to identify and implement appropriate security measures. The Comment further

stated that such 'process' must ensure the measures be continually updated in response to new technologies to maintain ongoing compliance with the ethical rules.

Other rules must also now be considered with cybersecurity in mind.

Additional rules also impose various cybersecurity duties. For example, Rule 1.4 imposes a duty to communicate with clients and obtain informed consent on critical issues, including whether special security protections are needed for a particular client to maintain the confidentiality of their data or communications. Rules 3.4, 4.4, and 8.4 relate to how lawyers deal with issues of metadata both intentionally and unintentionally communicated to third parties. Rule 5.3 makes lawyers responsible for their employees' compliance with the same ethical rules.

While these are the primary rules that have been explicitly identified as encompassing technological duties, it is important for attorneys to approach an analysis of any RPC with an eye toward technology and cybersecurity because, as explained below, the WSBA is doing exactly that.

WSBA Advisory Opinions shed light on the extent to which attorneys are responsible for maintaining adequate cybersecurity practices.

The Rules and Advisory Opinions often decline to adopt specific technical standards or particular thresholds. Instead, they place the burden of maintaining adequate safeguards upon the shoulders of the attorney.

Consider the issue of cloud computing. Many businesses, including law firms, have turned the storage of their data over to expert cloud-based vendors with access to the very latest security protections. In part, this is because contracting with a third-party vendor seems to take the burden of security off the shoulders of untrained attorneys and transfer it onto the shoulders of security professionals. This, unfortunately, is a faulty assumption.

The WSBA addressed cloud computing in Advisory Opinion 2215, announcing that attorneys retained the obligation to fully vet the cloud company, including its technical expertise, the details of how it transmits data, the technical adequacy of the security protections, even whether the servers are located in a place where relevant law supports privacy interests. The Advisory Opinion reasoned that because handling confidential paper records and practicing due diligence with vendors of law-related services has long been the responsibility of attorneys, cybersecurity matters should be no different. The obvious problem, however, is that we have undergone a paradigm change. Very little similarity remains between paper records, the old-school vetting of vendors and the new computing technologies.

The WSBA does recognize that many, if not most, attorneys do not have advanced technical knowledge but explicitly states that lack of technical knowledge may not be used as an excuse to fail to properly vet security vendors. The Opinion does list various 'best practices' to employ when vetting a vendor, including, "learn about data storage and read literature on risks, standards, and desirable features."

Additionally, the ABA's guidance on maintaining confidentiality amid cybersecurity challenges advises attorneys who lack technical competence and sophistication to partner with an outside attorney, law firm, or expert to ensure adequate safeguards are in place, and that third-party vendors are properly vetted.

Importantly, the Rules themselves assert that no civil liability arises from noncompliance. However, in addition to the risk of professional misconduct, the lack of formal regulation of cyber practices in the legal industry means that 'industry standards' and the 'reasonableness' of precautionary safeguards and responses to cybersecurity issues will likely be measured against the standards set by the Rules.

Direct Statutory Requirements on Lawyers

Like many businesses, law firms obtain types of private electronic information that fall within state and federal statutory protections.

Law firms are subject to Washington State's cybersecurity statute.

Washington State's cybersecurity statute, at RCW 19.255.010, protects 'unsecured' personal information of Washington residents held by any business or entity, including law firms. Such information includes social security numbers, driver's license numbers, account numbers, credit and debit card numbers, security codes, access codes, and passwords. Encrypted data, using acceptable protocols, is not considered unsecured unless the person gaining unauthorized access also obtains the encryption key or some other means of readily deciphering it. The statute requires notification to victims as soon as possible but not later than 45 days after discovery of the breach, unless it's not reasonably likely the victims are subject to a risk of harm. Notifications can be delayed by request from law enforcement. If there are more than 500 affected Washington residents the entity must submit a written explanation to the AG, which is posted to an online website. Enforcement can be through a private cause of action or by the AG, and the remedies of the Washington State Consumer Protection Act can be used.

Law firms can be subject to federal statutes.

Federal statutes imposing cybersecurity requirements are industry specific and law firms are generally not a directly regulated industry. However, law firms do partake in certain regulated activities. If the firm accepts credit cards it is subject to the cybersecurity restrictions of the Payment Card Industry Security Council's Data Security Standards (PCI DSS). If a law firm possesses Protected Health Information (PHI) relating to its employees, it must comply with the protections created by the Health Insurance Portability and Accountability

Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH Act). If a law firm is employed by the Department of Defense or another federal agency it may have to satisfy the cyber protections set forth in the Defense Acquisition Regulations (DARs) and the Federal Acquisition Regulations (FARs). If the firm has a pension plan it may be subject to the cybersecurity protections in the Employee Retirement Investment Security Act (ERISA).

Derivative Statutory Requirements on Lawyers

The final source of cybersecurity restrictions applicable to lawyers comes from particular clients they might represent. For instance, if a client is a health care entity it almost certainly falls within the reach of HIPAA and HITECH and thus acquires a catalogue of cybersecurity requirements aimed at protecting Patient Health Information (PHI). This is a high bar, including the necessity of a cybersecurity plan, enforcement mechanisms, and breach notifications. HIPAA also applies, however, to 'Business Associates' of the subject health care entity. 'Business Associates' might include law firms in possession of such information received from their clients. In other words, a law firm receiving PHI could be fully subject to HIPAA/HITECH along with the client.

And don't forget secure destruction. If a lawyer obtains certain consumer credit information concerning a client or others, for instance during discovery in a litigation, the Federal Trade Commission's disposal rules regarding electronic information may engage and control the destruction methods.

What to Do?

The primary means of dealing with cybersecurity, for lawyers and our clients, is to acknowledge it and put a plan in place. The twin goals of the plan would be to identify the applicable legal and regulatory duties, and the technical safeguards needed to meet them. Fortunately, the U.S. standard for such plans is set forth by the National Institute of Standards (NIST), and provides a 'best practices' approach explicitly acknowledging the need of plans to be fitted to an individual entity's size, types of electronic information, complexity of its data systems, and, importantly, its budget. It is not a 'one size fits all' requirement.

A NIST plan envisions a technical review of an entity's data handling and storage, devices, current security measures and vulnerabilities. It sorts out what works and what doesn't, and how to improve and protect the entity in the future. It typically includes an action plan if a breach occurs. Importantly, if there should be an investigation or litigation, the plan can be used to demonstrate efforts to comply with the legal standards of care and mitigate liability and damages.

The NIST protocols are not limited to private businesses and government agencies. They also fit the needs of lawyers and can be paired with ABA guidance and WSBA Advisory Opinions to ensure attorney compliance with the Ethical Rules and applicable statutes and regulations.

Cyber risk, the accompanying ethical and legal obligations, and the monetary and reputational consequences of failing to comply is absolutely worthy of attention, consideration, and a line in the budget. At the same time, these warnings ought not to panic attorneys. Cyber risk is manageable and adequate safeguards are affordable. But ignoring this topic is no longer an option.

Dedicating the time and energy to understanding attorneys' legal and ethical obligations is the first step. Seeking independent counsel may be justified because this is an emerging area of law where statutes and regulations often conflict. The second step is understanding the technical measures that can (and in some cases, must) be taken to meet those obligations. That technical review can be obtained directly from a cybersecurity firm or through independent counsel if needed.

Kurt Hermanns is 'of Counsel' at Gordon Thomas Honeywell, after a lengthy career with the United States Attorney's Office. He specializes primarily in federal criminal related risk management issues for South Sound businesses.

Amelia Whaley, a graduate of Duke Law School, is embarking on a clerkship with the Washington Supreme Court this fall. Most recently she has practiced as a dynamic commercial litigation attorney at Gordon Thomas Honeywell after serving as a volunteer investigator for the Colorado Public Defender, teaching English in Poland, and working for the Duke Clinical Research Institute. Amelia is an avid athlete, intrepid adventurer, and dedicated techie.