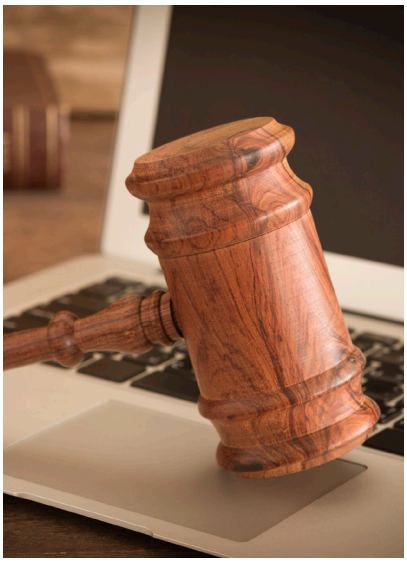
HA+W | Aprio
The new name for HA+W

Passionate for what's next

What is 'reasonable security'?

WHAT LAW FIRM MANAGING PARTNERS NEED TO KNOW

By Dan Schroeder, partner-in-charge, HA+W | Aprio Information Assurance Services



The legal profession has been a primary target for cyber actors for years. In 2008, a security firm discovered an advanced persistent threat (APT) that had been building in a law firm's network for nearly a year, allowing the attackers to harvest thousands of emails and attachments. In 2011, Chinese hackers infiltrated four Canadian law firms looking for inside information to derail a high-profile takeover bid.And the hits keep coming. The fact is, law firms represent an alluring honeypot for threat actors, whether their aims are financial, espionage or ideological. Here are a few examples of the high-value information that law firms often possess:

- Details of high-profile M&A deals
- Companies' trade secrets and other privileged information
- Information obtained from opposing parties in discovery
- Details of legal strategy in specific cases
- Tax records
- Bank account credentials

And yet, despite sitting on this veritable treasure trove of data, the legal profession has a reputation for being out of step with what are commonly regarded as effective and pragmatic approaches to cyber risk management.

Think you're the exception? Ask yourself these basic questions about your firm's cyber risk management:

- Can we identify the sensitive data in our custody?
- Do we understand the nature of the cyber threat to the firm?
- Do we know whether we have adequate safeguards in place to protect the data and fulfill our professional ethical responsibilities?

If you found yourself hesitating to say yes to any of these questions—or all of them—don't feel too bad. You are in very good company.

Cyber risk management requires a logical, risk-based approach that demands executive-level involvement. It is not something that you can "throw over the fence" to the IT department.

Faulty assumptions about cyber risk

Despite the fact that safeguarding confidential information pertaining to their clients is central to lawyers' ethical standards, few law firms have formally assessed the potential threats to electronic information, much less put in place an appropriate cyber risk management program. We have a few thoughts on why:

- First, many law firm managing partners mistakenly assume that this is an IT matter and the IT organization has this covered.
- They may believe their firm is too small to be a target.
- The problem is too complex, and there is no roadmap on how to address it.

This last faulty assumption truly gets to the heart of why most law firms are turning a blind eye to their very real and potentially devastating cyber risks.

But here's the rub: ignorance is not bliss. Whether or not your firm discovers that it has been breached (and most security breaches go undetected for months or years), it's only a matter of time before cybersecurity comes up as a factor in obtaining or retaining significant business accounts.

Especially in highly-regulated industries such as financial services and healthcare, businesses increasingly demand assurance from their third-party service providers about how they understand and manage cyber risk. These vendor management roadblocks often can prove even more onerous than regulatory ones. Just ask anyone in the burgeoning financial technology ecosystem.

Not paint-by-numbers

The good news is that cyber risk management does not have to be complex—and, in fact, there is a roadmap for addressing it. It's just not a detailed, paint-by-numbers map. Instead, cyber risk management is a logical, risk-based approach that demands executive-level involvement. In other words, cybersecurity is not something you can "throw over the fence" to the IT department.

There is one concept that is central to every significant regulatory standard on cyber-security. That is the concept of what is "reasonable and appropriate." As stated in the American Bar Association's Cybersecurity Handbook: "[T]he standard for compliance, if one is stated, is typically that security must be 'reasonable,' or appropriate.'"

The legal definition of "reasonable security" has rapidly evolved from a notion of specific security measures that are deemed adequate (passwords, firewalls, vulnerability management, etc.) to one of a risk-based management process. This "process-oriented approach" to cyber risk management is becoming the standard of care for state, federal and international regulators.

As stated in the American Bar Association's Cybersecurity Handbook: "[T]he standard for compliance, if one is stated, is typically that security must be 'reasonable,' or appropriate.'"

Focus on value at risk

Here's some more good news: You don't have to boil the ocean to manage cyber-related risk. But you do have to spend the time up front to understand what is truly at risk. As outlined in the ABA's Cybersecurity Handbook, the process-oriented approach to cyber risk management looks something like this:

- **Identify digital assets.** Effective cyber risk management must begin with understanding the relative value of your firm's digital assets—those data elements that enable your business model—and the business impact if those assets were compromised.
- **Conduct periodic risk assessments.** A thorough inventory of information assets provides the foundation for a targeted cyber security risk assessment, which will assess the "value at risk" those digital assets represent to the business.
- **Develop and implement an appropriate security program.** This asset-based approach allows your firm to focus its information security, money and resources in the most cost-effective way—selectively applying advanced security measures to higher value assets, while maintaining baseline controls for the majority of data.
- **Ongoing monitoring and reporting.** The final piece of this security program involves regular monitoring and reporting to drive improvement and provide assurance to your trading partners that you are doing the right things to protect their interests.

A manageable approach to cyber risk management

Whether your firm is one of the Global 200 or a small, boutique practice, understanding and managing cyber-related risk is not only a business imperative, but it is also 100 percent manageable.

A realistic assessment of threats to digital assets, followed by appropriate treatment of those risks represents not only an efficient approach to cyber risk management, but also increasingly is the standard by which your firm will be judged. Ultimately, this risk-based approach is your best bet for protecting your firm from potential liability.

About Aprio

Since 1952, clients throughout the U.S. and across more than 40 countries have trusted Aprio for guidance on how to achieve what's next. As a premier, CPA-led professional services firm, Aprio delivers advisory, assurance, tax and private client services to build value, drive growth, manage risk and protect wealth. With proven expertise and genuine care, Aprio serves individuals and businesses, from promising startups to market leaders alike.

Aprio.com

Morison KSi
Independent member

For more information about Aprio's Information Assurance Services, contact:

Dan Schroeder
Partner-in-Charge
Information Assurance Services
dan.schroeder@aprio.com
770.353.8379