Assessing Your Law Firms' Cybersecurity Preparedness

Creating genuine partnerships to mitigate risks

__Augustin Cal__ and __David Sankar__, both in product management at __Wolters Kluwer's ELM Solutions__, have spent a good deal of time recently thinking about collaboration. And not just the kind that they bring to their workplace (and to this interview). It's the kind that law firms and law departments need to learn – separately and together – if they hope to create a cybersecure environment in which to work. As it happens, in September, Cal and Sankar's company introduced a new application that's designed to assist them in this effort. The interview has been edited for style and length.

We see almost constant news stories about cybersecurity attacks and breaches. Why are law firms particularly vulnerable to attacks and data breaches?

Augustin Cal: Many law firms are lagging behind when it comes to technology. At the same time they are in possession of very sensitive data. This makes law firms a high-risk target for cyberattack. Many law firms don't take adequate security measures to safeguard confidential client data. Too often we hear about very basic steps that are not being taken: for example, maintaining current patch levels on software or encrypting data. Given all this, it has become increasingly important for companies to implement cybersecurity assessment programs geared specifically toward law firms. The assessment is intended to let the clients know where each of their law firms stand in keeping their data safe.

How are law departments handling the cybersecurity risks inherent in their law firm relationships?

David Sankar: There's greater recognition among legal departments, more than ever before, that law firm cybersecurity risk is critically important to the legal function, and it's more than an IT-only responsibility. Historically, cybersecurity risk management was identified as solely an IT task, but there is no doubt today that it requires a legal and IT partnership. Our experience at Wolters Kluwer's ELM Solutions is that there are varied approaches to how legal departments manage cybersecurity risk.

Understanding that cybersecurity is an urgently emerging risk for the legal function, the default response to managing it is and continues to be through spreadsheets and email. It's kind of a first reaction: When there's a need, you go to what's familiar. And for many people, emails to law firms and managing data in spreadsheets are familiar. And that's OK as long as there is a plan simultaneously being formalized to implement a law firm–specific cybersecurity assessment program.

Emails and spreadsheets are not a viable long-term substitute for purpose-built software. When you look at more mature cybersecurity risk management approaches, you see a full partnership between the law department and information technology and security departments. In addition, purpose-built software is being used to create and manage assessments, to track and analyze the results of the assessments, and to create and take actions on remediation plans. We've also seen in some of these more mature programs that companies will partner with third-party consultants in order to execute on these assessments.

Cal: Also, a law department will tailor a program based on risk level. They may judge that some firms require something different than others. Let's say, for example, there is a mergers and acquisitions firm working on a sensitive M&A project. That firm should not be surprised if they are asked to answer more questions for that client than some of the other firms.

So what are the key elements law departments should focus on to obtain comprehensive cybersecurity readiness?

Cal: It's important that law departments recognize that managing cybersecurity risk is not just a one-time event; it's something that needs to be ongoing. I'd like to zoom in on a few key elements related to comprehensive law department cybersecurity readiness. The legal function needs a formalized assessment program in place that includes recurring surveying of law firms with the flexibility to assess off-cycle, as required by a cybersecurity event or a change in IT policy. Legal departments need purpose-built assessment technology – the right technology is critical for program success. Technology should automate the workflow internally as well as externally with law firms. Legal departments along with their IT partners need a solution that will provide a secure medium for transmission of assessments and related data.

Sankar: Just a couple other key elements to add – one being content. It's important that law departments and their internal partners, typically information technology and security, have risk assessment content that is specific to law firms. The interactions and the data sharing often differ between legal departments and law firms, as compared to nonlegal vendors. It can vary from law firm to law firm, based on the type of work that is being done and the sensitivity of the work.

Also, when you're looking at implementing a cybersecurity program, you can't boil the ocean. Many companies have hundreds if not thousands of law firms that they do business with, so it's important to take baby steps and say, "OK, where am I going to start with my program? Which firms am I going to assess?" Initial assessment program efforts may start with preferred firms, since the majority of legal work is often routed through preferred outside counsel. It may start with a subset of that firm list or with those firms handling your most sensitive work.

David Sankar *is an attorney and senior director in product management of the growth portfolio of Wolters Kluwer's ELM Solutions. He leads a team responsible for identifying, prioritizing, validating and incubating new growth markets. In this role, he oversees the introduction of new growth products and services along with managing the law firm product portfolio. He joined the company in 2010 and held positions in operations, sales and services before assuming his current role. He has extensive experience and a passion for working with legal professionals to drive technology value, solve challenges and create operational efficiencies. He can be reached at David.Sankar@wolterskluwer.com.*

Augustin Cal *is a product line director in growth markets at Wolters Kluwer's ELM Solutions. He is responsible for determining how the company can best serve new markets, defining strategy and executing on those plans. He works closely with customers to understand their needs and find new ways to help them overcome challenges that are not yet being addressed by their existing solutions. He joined the company in 2006 as a member of the software engineering team before moving into product management. He can be reached at augustin.cal@wolterskluwer.com.*

Many law firms are lagging behind when it comes to technology.
–Augustin Cal

The takeaway is to have content that's geared to law firms and focus on those law firms that you're doing business with in the most sensitive areas.

The last key element, and maybe the most important, is collaboration – both internally and externally. Successful collaborations between the law department and information technology and security teams are the foundation for creating seamless interactions with law firms that foster compliance with company IT policy.

Can you expand on the role of collaboration?

Sankar: Many organizations excel at securing their internal walls from cyberattack. Securing data that sits outside of their walls: This is where the collaboration really comes into play. Effective cybersecurity readiness programs demand collaboration between Legal and the information technology and security teams. Those teams have to be able to share information effectively and collaborate with law firms to be certain that all Legal and IT-related cybersecurity policies are included in assessments, ultimately ensuring that law firms are complying fully with all policies.

Cal: In addition, the law firms need to be transparent and open with clients when they are not compliant, and inform the clients as to the steps they are taking to become compliant. Ultimately companies select law firms with good reason, based on their legal expertise. So it's in both the client's and law firm's interests to work together on cybersecurity to meet the necessary compliance requirements.

Tell me what Wolters Kluwer's ELM Solutions is doing to assist companies working with their law firms on cybersecurity readiness?

Sankar: We recently introduced our Cybersecurity Risk Assessment application. It facilitates the internal and external collaboration needed to manage cybersecurity risk as it relates to law firms and other legal service providers. More specifically, the application provides workflow capabilities that aid in the delivery and review of law firm assessments, as we've been talking about today. It also allows users access to all assessment data and related documents that have been submitted by law firms, subject to application security framework, of course.

The application provides a secure medium for assessment collaboration between companies and their firms, and it includes the ability to capture remediation plans and document actions and the status of such actions. Much of what we've talked about today in terms of collaborations, assessing law firms and content can be managed through this application and in a secure environment.