Question: In the wake of prominent vendor security breaches, including at LexisNexis and Wolters Kluwer, as well as law firm breaches, what security concerns keep you up at night and how do you stay abreast of best practices in information security?

When the network goes down, work grinds to a halt. This has been true for at least a decade (probably two decades), and we joke at our offices that when the network goes down, it is the only time you’ll see some attorneys actually leave their office and talk with their work neighbors. For years, we worried about internal or physical issues such as a server crash or if a farmer cut a network cable in Nebraska. Such issues tend to be far less of a concern these days than a ransomware attack that can wipe out your entire electronic dataset and put you in the headlines due to state data breach notification laws. That definitely keeps me up at night.

The biggest issue that we face is the number of resources we access on a daily basis that require the use of a username and password. Many of these resources use single authorization access, and to no one’s surprise who is...
reading this, passwords get reused, and sometimes shared. We currently encourage, but don’t require, that our employees use password managers to prevent overuse or easily cracked passwords. I use Dashlane to manage my accounts, both personal and professional. We also encourage vendors to use two-factor authentication techniques to access their products, as well as their personal accounts such as email, Facebook, and Twitter. While two-factor authentication can slow down access to resources, it is a fair trade-off for preventing a breach of our data or computer systems.

Our IT team now has dedicated security experts on staff to help us understand new threats, and to help save us from ourselves. There have been horror stories of other firms who found out, the hard way, that unvetted software from countries like Ukraine, Russia, and/or China have malware embedded in the code, which can be activated at a later date, or can just continually siphon off personal or client information for years. While we want to be nimble in our operations, it is extremely important to have software and online resources cleared by our security teams before granting staff access to our secure information.

Law firm clients are not just trusting us with their data anymore. Clients, especially those who are in regulated industries, make their external law firms go through security audits to make sure they are following best practices with their data. These are stringent processes and require that we constantly educate our attorneys and staff on potential threats and proper methods of handling client data.

Finally, it is up to everyone to understand current threats regarding information security. Read those alerts from your security team. Follow guidelines set by your organization. If you are interested, there are podcasts such as Hacking Humans and Security Now that discuss new threats and give good advice on handling information security. If you’re short on time, Internet Storm Center’s Stormcast is a quick five-minute podcast that keeps you up to speed on new threats. We are all under attack, so it is everyone’s job to identify potential security issues, and to not be the reason that the network goes down.

Another big concern related to any kind of security breach is the risk of service disruption. Any loss of use of a service, especially one that affects a large research platform, will have serious consequences for end users who rely heavily on that service. What we can do is work with our IT group by sharing information on risks and advising them on risk avoidance/mitigation. Having sound, credible information on those threats—and taking actions to protect against them—can play an enormous role in helping to ward off those who seek to profit from network intrusions. For me, the most effective way to do this is by networking with my peers.

Listening to, and sharing, what we are all doing is exponentially more informative than anything any one person can do to keep abreast. Nothing beats learning from someone else’s knowledge and experience, especially if that person is an expert who has already figured out what works best. Reading reputable industry press releases and curated news alerts from our research team are also excellent ways of staying informed.

Although our IT group has the primary responsibility of keeping the firm’s network safe and secure, security concerns are nevertheless an inescapable reality for directors of research services because of our extensive reliance on electronic subscription services.

One such concern, with serious implications, is that we would have to deal with the likelihood that compromised data can be used in ways that can cause reputational or financial harm to our clients, our firm, and our end users. Those concerns stem from the information (e.g., names, locations, etc.) we share with electronic subscription services and the information those services collect and store from our end users, such as search strings, search history, etc.