Bloomberg BNA

BNA's
Corporate Counsel Weekly™

Data Security and Law Firms: How to Stay Ahead of the Curve

Bloomberg BNA recently conducted this interview with Jason Parkman, CEO of Mitratech, about data security and how law firms, and companies, can best protect themselves and their clients.

Bloomberg BNA: What is the ''industry standard'' in regards to data security, and why has the legal industry generally remained below this standard?

Jason Parkman: The industry standard for data security these days is for every company to have policies that get followed consistently by all of their employees and to not allow for unencrypted data to be sent via email. Law firms have not consistently lived up to this standard in part because of the close relationship they have enjoyed with their corporate counsel. They have, in many ways, viewed their relationship with corporate counsel less as a business relationship, and so in some sense, not subject to the traditional business constraints as a company like Mitratech or any other software vendor would be. Instead, it is viewed as more of a counseling relationship. I think it's a vestige of past relationships that is certainly changing.

BBNA: Citigroup's cyberintelligence center recently released a report stating that it was reasonable to expect law firms to be targets of attacks by foreign governments and hackers; how do law firms protect themselves from these types of sophisticated hackers?

Parkman: Some law firms use the industry standard protection mechanisms, whether that be industry standard hosting of client data, industry standard encryption of client data, or policies and practices around not using email to send and share client data. There are certainly some law firms that treat the data with the same level of control and protection that any other company that's in the data business would treat data with. In fact, in some sense, law firms are in the data business.

The larger point is that it's not consistent. Not all law firms really expect that same kind of level of control over their client data—I think that's where the issue arises. Any other company that hosts a lot of sensitive data for a particular client, as often happens with law firms, would be subject to extremely stringent data protection requirements. There are some law firms that abide by strict data protection requirements, but it's not the case that they all consistently do.

I think anyone who is not following all of the industry best practices is vulnerable. Also, if the weak point of companies who may be targets of hacking and attacks is their law firms, that's going to make the law firm more of a target. It's not for the law firms' own data—it's a back door into the corporate data.

BBNA: The FBI and top federal prosecutors at the Department of Justice have been urging law firms to be more open to reporting data breach incidents. Why does the legal industry seem to be so reluctant to sharing this information?

Parkman: As private companies, law firms are subject to some different rules than other companies are. They are even subject to different rules of ownership because we don't have the same legal services act that the U.K. does. Large law firms, or law firms in general, have enjoyed a certain level of ability to protect their information. Regulators and prosecutors are suggesting they no longer enjoy this protection, and I don't think they're happy with the suggestion that the rules change on them.

BBNA: What's at stake for corporate clients whose sensitive data is hacked?

Parkman: What's at stake is regulatory scrutiny, extensive fines (especially as we look at international firms divulging corporate secrets), and the loss of personally identifiable information to name a few things. Not to mention intellectual property, which is in many ways the core value of so many companies these days. The stakes are tremendously high which is why you see data protection and data privacy issues in the news so frequently. If you have the ability to lose, potentially, hundreds of millions of dollars in direct fines, as well as intellectual assets and the trust of your

Jason Parkman is the CEO of Mitratech and has more than 15 years of experience leading legal technology, software and services businesses. In the three years since Jason joined Mitratech, his team has produced the strongest years of growth and client success in the business's 27 year history. Prior to Mitratech, Jason served as Senior Vice President, Large Law Firm Business at Thomson Reuters, General Manager of Hubbard One, a fast-growing legal software business, founder and CTO of Juritas, an innovative online legal document business, and Director of Technology Development at litigation powerhouse Bartlit Beck Herman Palenchar & Scott.

 ISSN 0886-0475

clients and the public, I'd say pretty much everything is at stake.

BBNA: What proactive measures can corporations take to protect their sensitive information when they share it with outside counsel and third party vendors?

Parkman: Ensure that a non-negotiable part of your relationship with those outside counsel or third party vendors is that they follow industry best practices, that they enumerate those best practices, and that they agree to live by those best practices, just as you would any other company that houses your data. Don't consider the law firms to be in a special situation because of their ''counselor'' relationship. That's probably the biggest lesson: expect the exact same thing from a law firm vendor as you would from any other vendor who has access to your sensitive data and will store it on their servers and may communicate it.

The fact is, industry best practices are changing practically daily. Companies like Mitratech are required to keep up. They need to get certified, have third party intrusion detection, and lift certain levels of encryption when housing data. Law firms should be expected to do no less, and if I were a client of a law firm in this type of situation, I would expect that they would live up to those same standards in order to use their services.

BBNA: How can law firms ensure that the sensitive information they share is protected?

Parkman: I think the most important thing to recognize there is that law firms are in the data business. They are in the business of managing, housing, sharing and making decisions based on client information. It's an information economy, and law firms are at the center of it. As such, I would say they should look to other companies and understand what it is that those companies are doing who see themselves in the data and information business. Then they should hold themselves to those exact same standards.

BBNA: How does the increase in law firm hacking affect the relationship between corporations and their outside counsel?

Parkman: We're seeing a larger trend of corporations and law firms starting to change their relationship to more of a business relationship. From the choice of outside counsel based on financial metrics and results more than based on past relationships, to procurement processes where the law firms have to get involved in procurement processes and reverse options, the relationship which has been a historical artifact is changing. It is becoming much more like a typical vendor-client relationship.

I think what we're seeing around this set of questions is that one of the things that needs to be dragged along as that relationship changes is the expectation of how information and data will be stored. Law firms need to fully recognize that they are businesses, run themselves like businesses, expect to be treated that way, and expect to be held to the same standards.

CCW ISSN 0886-0475