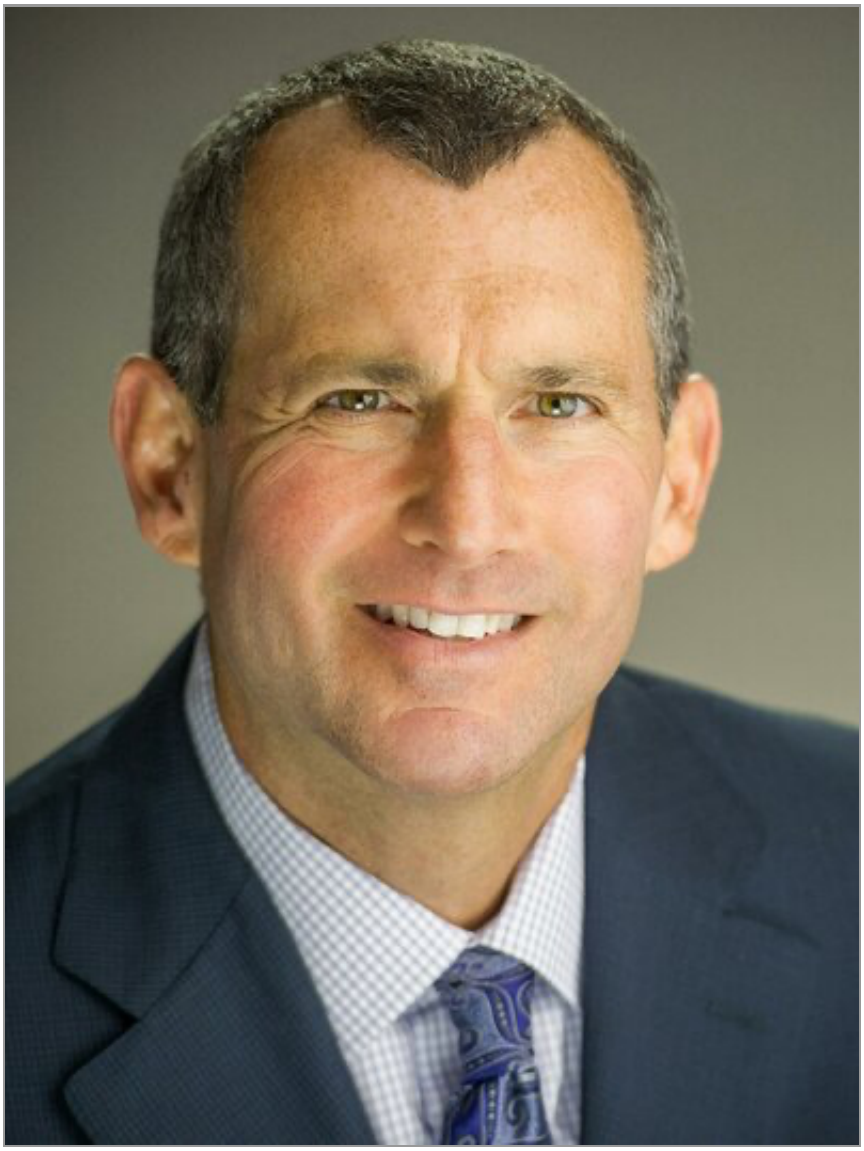
Law360 Pulse
A LexisNexis® Company

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Ex-SEC Internet Office Head On Cybersecurity's Future In Law

By **Anna Sanders**

Law360 (February 24, 2021, 10:48 AM EST) -- Remote work during the coronavirus pandemic has only reinforced the importance of cybersecurity at law firms and legal departments for attorney and consultant John Reed Stark.



John Reed Stark

At John Reed Stark Consulting LLC, the former U.S. Securities and Exchange Commission attorney advises law firms and other organizations on how to avoid and respond to data breaches and other cybersecurity incidents that put lawyers and their clients at risk.

Before starting his own consulting firm, Stark served at the SEC for 18 years, including 11 as the founder and chief of the agency's Office of Internet Enforcement. He was an adjunct professor at Georgetown Law for 15 years, teaching a course on law, regulation, cybercrime and technology, and he worked as a managing director of risk management firm Stroz Friedberg LLC. He even taught sessions on cybercrime at the FBI Academy and is a senior lecturing fellow at Duke University School of Law.

Here, Stark talks about why law firms need to prepare for the inevitability of data breaches and other incidents in the increasingly tech-driven workplace, as well as the future of the cybersecurity field. This interview was conducted Feb. 16 and has been edited for length and clarity.

You went to law school and were an attorney by trade. What made you decide to go into cybersecurity?

I left law school and joined a law firm and then I was in D.C., so I wanted government service somewhere. I always loved securities and investing, so I joined the SEC. I ended up doing cyber at the SEC at a very early time, starting in 1994. And then in 1998, I became chief of the Office of Internet Enforcement and did that for 11 years. Most people when they leave the SEC, especially the division of enforcement, they go to law firms or they go to work for a financial institution like a bank or a brokerage house. I was more interested in the juxtaposition of business, law and technology. There was this extraordinary firm called Stroz Friedberg that brought those three disciplines together. Most of what I do, it feels like I'm practicing law, but I'm not. The area of data breach response, when I joined Stoz Friedberg, was just developing as a real practice area for lawyers and now it's really exploded. It's an extraordinarily exciting time for lawyers who do data breach response work.

Why is that?

The workflow for data breach response has become so complex and so litigation-minded — there's regulatory inquiries, law enforcement liaison work and, of course, investigations and statutes that are state, federal and international when there's any sort of data security incident. And there's multiple disciplines within that — retail, financial firms, health care organizations — all of those trigger different statutes, so it's really become an area where the quarterback of any incident response is now, most often, the attorney, because everything a victim company does has such extraordinary legal implications.

How does your work intersect with the legal industry?

It constantly changes. But generally you're engaged by the law firm and you're part of the team of experts that's advising the law firm in helping them defend a company against the onslaught of litigation, regulatory and other legal implications after a data breach. That has changed dramatically over the last few years. The law around keeping the work that you do confidential, and within the context of the attorney-client privilege, as an entity that provides services for the law firm has changed.

What are the biggest threats to a law firm's

cybersecurity?

The number one threat is that so many lawyers are now working from home. Lawyers operating in law firms, their number one priority is not necessarily going to be making sure they practice good cyber hygiene. Instead, it's going to be responding to their clients, which is, these days, a 24/7 requirement. So lawyers are under extraordinary pressure from their clients to respond quickly, the legal marketplace is fiercely competitive. In responding quickly they might not necessarily use a device that has the best security, might not use a means of communication that is necessarily the most secure or just, again, through the excitement and enthusiasm and passion in responding to a client, might forget to be careful with respect to their cyber responsibilities.

And that's exacerbated by the realities of remote work during the pandemic?

Right. It's both the applications being used, the devices being used, the connections being used — all of those different areas can be exploited by threat actors. The dynamic of the threat keeps changing every year. It's a very exciting area to work in because of the demand. I always feel like I'm a plumber the day after a hurricane. That's how much in demand my services are — because it's really an area that most companies are not familiar with, they haven't been through it before, they're not sure exactly what to do when they get hit by a ransomware attack or they get hit by some sort of advanced persistent threat.

Remember, legions of soldiers are waking up every single morning with the sole intent to hack into U.S. systems. That's a very formidable enemy that just keeps growing more and more tech-savvy. And with the use of cryptocurrency, but Bitcoin in particular, the threat actors from around the world have a very easy means of extorting payment from their targets and a very easy means to profit anonymously. The dirty little secret is that companies often pay the ransom and it's very rare that a ransomware attacker is actually caught and apprehended and brought to justice and extradited.

What mistakes do law firms make when implementing cybersecurity measures?

Small firms, medium sized firms, large firms all have different types of problems and all have different levels of resources they can use to address those problems. But across the spectrum of every single law firm I've ever worked with, there are three things that I think law firms typically don't do well.

One, they aren't up-to-date on their cyber insurance. The cyber insurance market has changed dramatically. Historically, cyber insurance policies were bespoke, but now there are certain endorsements and other important provisions of cyber insurance policies that law firms should make sure they have, and it's very critical to stay up to date with those types of provisions. I find that my clients don't necessarily know what's covered and what's not in the event of a cyberattack or any data security incident.

Number two, there's historically been this tendency, especially from law firms, to do what's called "penetration testing" and think that meets their requirements for an independent assessment of the robust nature of their infrastructure, of their governance. There's no silver bullet for data breach and it's not a matter of if but when. Cybersecurity is an oxymoron. You are going to experience an attack and it's all about how you respond. I think firms can be a bit too myopic in their approach. They might not hire a truly independent firm that will give you the good, the bad and the ugly with respect to a true risk security assessment that doesn't just look at your technology but also your governance and gives you a holistic approach toward your overall cyber

awareness.

Number three is personnel and capital associated with cybersecurity generally. It's a remarkably competitive marketplace. There are three or four million vacancies in the cybersecurity space right now, so competition for getting good people is very difficult. Keeping those people and paying them enough and creating an environment that works for them is always a challenge because they are always a phone call away from leaving you.

What's a cybersecurity assessment and how can it help law firms?

Cybersecurity assessments really change depending on what software you're looking for. Generally, it's a holistic look at both insider threats and external threats, the applications that you use, the current infrastructure that you use, and, most importantly, the current governance that you have to make sure that you're doing the best with what you have in terms of resources. I can always come in and give you a heat map or a laundry list of things that need to be improved. But you have to be realistic within a business model, and you have to be mindful to not to create a roadmap for future litigiation.

For example, a big part of a law firm's market and the most important part of their website are the biographies of the lawyers who work at the law firm. And those biographies have extraordinary information on them, they're very, very detailed about the accomplishments of each lawyer, where they've worked, maybe the cases that they've worked on, maybe the clients that they have, where they went to law school. It's a treasure trove of phishing information. So if a hacker wants to somehow bamboozle a lawyer into clicking something at 4 a.m. when they're trying to respond to a client, it's not going to be that difficult to socially engineer that email, because there's so much available in that biography that will allow someone to really customize their spear phishing expedition and get a lawyer to click on something they shouldn't have. It would be totally unrealistic and absurd for me to tell a client they can't have these biographies, because that's a major part of their business. So you have to figure out a way to work around that and to be realistic with respect to the lawyers' existing business model and the types of recommendations.

As part of an assessment, you're certainly going to be looking at the most recent specific kinds of threats and exploits, as well as governance. The tools don't matter if you don't have good governance. For example, you might have an extraordinary end-point detection and response tool that sends out all sorts of amazing alerts to tell you when there's something unusual or suspicious going on in your system. But those alerts are not worth anything if you don't have a governance system that, first of all, modulates the settings on those alerts so you're not getting a thousand a day, and second, establishes a reliable system to manage and respond to the alerts.

What do you see as the future of cybersecurity in the legal industry?

It is probably the most exciting dynamic and entrepreneurial area to practice law. Because privacy is so dynamic and changing, because the threat, both external and internal is changing, the lawyers involved in this kind of practice are typically a little different. Their pathways have been different, some of them are former prosecutors, some of them are former intellectual property lawyers, some of them are former engineers, some just fell into this because they were advising the client and the client had a big breach and they learned by doing.

Two or three years ago, law firms didn't really have a separate privacy and incident response and cybersecurity practice. Now law firms are building these really big practices and you're also seeing

incredible movement, incredible mergers and acquisition movement in the consulting business of law. There's now law firms that only do cyber, which is very unique, and there are law firms that only do privacy. That's incredibly exciting because those law firms are growing, doing interesting work and really sort of carving their own way, making their own path.

You're also seeing incredible private equity interest and corporate interest in the various consultant firms that do cybersecurity and that's sort of spilling over into the law firm practice as well. There's incredible competition. If you're one of those people that doesn't necessarily fit in that law firm environment and you're looking for something different, there are so many ways to go now in terms of cyber.

--Editing by Alyssa Miller.
