TELL US MORE

LISA SILVERMAN '89: Corporate Investigator

PHOTO: MATTHEW GILSON

Lisa Silverman's work is all about finding the proverbial smoking gun. As managing director at global corporate-investigations firm K2 Intelligence, LLC, Silverman, who is based in Chicago, conducts multinational investigations for clients usually looking to identify bad actors in high-stakes white-collar dealings.

Silverman has been in the business for two decades, first working at Kroll Associates, the firm credited with originating the modern corporate-investigations industry. (Founder Jules B. Kroll sold that company for $1.9 billion and launched K2 Intelligence with his son Jeremy in 2009.) During those years, she's seen it all—cybercrimes; trade secrets spirited overseas; a range of frauds, including early signs of some major headline-making scandals; and a variety of international compliance issues with no easy solutions. Silverman's job is to follow the trail of clues to the bare facts, and then to help her clients use them in a way that leaves them as whole and protected as possible in the corporate and legal arenas they occupy.

She's rare in her industry—a veteran woman investigator in a field dominated by men with law enforcement on their résumés. But Silverman draws strength from her eclectic background, which includes her Haverford B.A. in history and women's studies, an M.A. in European history from Columbia University, and an M.B.A. in finance and international business from New York University. Before becoming an investigator, she worked for *Sesame Street*, developing curricula for the show. The connecting thread, Silverman says, is her ability to observe and think critically—key skills that she has sharpened every step along the way.

You don't have the typical background of a corporate investigator. To what do you credit your success in the field?

I think learning to read and write and think prepares you for just about anything.

I work with people who think, "You need a career in law enforcement or you need a degree in business." I can teach you how to crunch numbers and how to read a piece of litigation, but I can't teach you how to think critically about what you are reading and see how it fits or doesn't fit into a larger pattern of facts.

I tell people all the time how well my Haverford education prepared me perfectly for this job—particularly my junior and senior history seminars. *The Historian As Detective* [one of the texts] sits on my work bookshelf.

There are many TV shows that deal with white-collar crime. How do you describe the reality of what you do as a corporate investigator?

It's rare my daily life feels like TV. And I can assure you that undertaking surveillance is nowhere as sexy as it looks. Really, I help clients, mostly corporate clients, but sometimes government clients, make decisions based on uncovering the facts of what has happened or the risks of what might happen.

So, as a company, the question may be "Do you want to get involved in something?" Or sometimes it's "How do you clean up something that already happened?" My job is to find out the facts so that my clients can determine what to do going forward.

The hardest thing about my job is to not try to make my facts stick to theory, but to develop a theory based on the actual facts. Clients sometimes have a theory about what happened … everybody has a story. But my job is to find the accurate story, not just the popular one.

What kinds of situations do your clients bring to you?

I usually get involved in one of two ways, either pre- or post-incident. Pre-event, a client might say, "I'm thinking of getting involved with another company, but I don't know that much about them." Or, "I do a lot of business overseas and I'm worried about protecting my data from hacking."

I say to clients all the time, "It's way better for you and much more cost-efficient if I get involved pre-event." With post-situation problems, the client is often in crisis mode. Those are: "We discovered an employee has embezzled money"; or "We had proprietary information hacked from our network and we have to respond"; or "The Justice Department says we have a Foreign Corrupt Practices Act issue in China and we have to deal with it."

Tell us a little more about that last scenario.

The Foreign Corrupt Practices Act, or FCPA, is a U.S. law that prohibits the payment of bribes to foreign officials to obtain or retain business. It also requires companies to maintain accurate books and records. What it means for U.S. companies is they can't pay a bribe—no matter what the laws and customs are in another country. But [in some countries] "facilitation" payments are considered part of doing business, as are other practices, such as doing favors for family members of elected officials. Although the laws are absolutely clear, it's sometimes difficult for a company to control what's happening remotely, and that's how FCPA violations occur.

You mentioned networks and hacking—how much has the growth of the internet affected what crosses your desk every day?

When I started in this business, just being able to get information set us apart from most firms. Knowing where repositories of information existed often ensured success in an investigation. But, with the ever-increasing amount of information available on the internet, getting the information is just the first step. Where my skills come in now are in undertaking a thoughtful analysis, separating accurate information from falsehoods, and then determining how the information fits together to tell a story. It really is the historian as detective. Also, the repositories for information have changed. When I started, if we were investigating an employee for fraud, it was common for us to go in [to an office] at night and go through files. I can't remember the last time I did that. Instead, we forensically image the subject's computer and conduct our analysis digitally.

Does that cut both ways? How has corporate crime changed with the advent of social networks and the internet?

It's hard to believe that social media as we know it has really only been around for a little more than a decade. LinkedIn was started in 2002, Facebook in 2004, Instagram in 2010, and Snapchat in 2011. So, not surprisingly, social media as a legitimate source for investigation and for trouble has grown. Employees need to think really carefully about going home and saying [on a social network], "We're working on this great project at work" and describing it, because they may be leaking confidential information. Similarly, things a friend posts about your activities could come back to haunt you later on, particularly as employers pay more attention to what people are posting. Also, although there are more safeguards around confidential information, if it's leaked or stolen, what happens can be far more significant. You've seen it with WikiLeaks, and you see it in some of the data breaches we've had recently.

I was involved in a situation about two years ago where a client hired a temporary employee and gave the temp the password [of the person being replaced, who had access to everything at the organization]. The temp, who had a criminal record, used the password to steal confidential information. I was brought in to help the client figure out how many people might have had their information compromised and what that would mean for the client—not so different from what happened in the Target data breach. In that situation we had a great outcome. Through computer forensics, we were able to definitively show what files the temp had accessed, and it turned out to be less than a dozen people, rather than thousands of possible victims.

You stumbled on some evidence of a major fraud before it hit the news. Tell us about that.

What's really fun for me is when you are looking at what you think is a known quantity but you are doing it with fresh eyes and you find something that makes you say, "Wait, that can't be right." A bunch of years ago, I did an investigation like that for a corporate client who asked us to have a pro forma look at someone they thought was issue-free. I can't name him, because of legal issues, but we didn't just read the press, we looked at a number of primary-source documents and found information that didn't make any sense in the context of what we thought we knew. Our client didn't do the deal, and less than a year later the individual was indicted and convicted of major fraud charges and is now in jail. That was a great case, and the client walked away from the deal. Of course, there are clients who don't take my advice, too.

What would you change about your industry?

Despite the fact it's 2016, it's still an incredibly male-dominated industry, particularly at the senior levels, and it's something I feel and think about all the time. As one of the few senior women in the industry, it's really important to me to mentor women coming up in the field. Part of that is helping them find their voice and their confidence. Particularly, as a woman, you can't go into a meeting and "uptalk." Say what you know, don't ask it. You have to go in with a swagger of confidence, even if you don't believe it, because you're a female in a room full of men and it can be harder to be heard in the same way. —*Michelle Martinez*