CyberInsecurity News™
WHAT LAWYERS NEED TO KNOW

FEBRUARY 2019

INTERVIEW: SANDRA JESKIE / DUANE MORRIS

SHE SPEAKS LEGAL, BUSINESS AND TECH TO TALK CYBERSECURITY

It can help to be trilingual as you guide your clients through these perilous worlds.

*There can't be many lawyers who followed the career path that **Sandra Jeskie** did on her way to becoming a partner at Duane Morris. Her work experience and her education took her in directions that seemed far away from a career in the law. But as it turned out, she built her practice around those pieces, and she is now convinced that the success she's enjoyed as a lawyer is directly related to the journey along the way. And the beneficiaries, she says, are her clients.*

CyberInsecurity News: *When did you first start thinking you wanted to be a lawyer?*
Sandra Jeskie: From the time I was a child I wanted to be a lawyer, but my path was not direct. I worked full-time, beginning when I was in college, and I also earned a graduate degree while I worked, before I transitioned into law.

CN: *You worked at Computer Sciences Corporation. What did you do there?*
SJ: I am very analytical, and I had an interest in math and science. I began my software career at Sperry Univac as a programmer, and then spent 15 years working at CSC, leading teams of software developers.

CN: *After college, you shifted your focus. But it wasn't to pursue a career in law.*
SJ: After obtaining my B.A. in computer science, I took evening classes toward a master's in electrical engineering, with an emphasis on computer design. But before I completed the EE degree, I made my first big pivot. I moved into an MBA program. I thought this would be a good addition to my background. And I was right. Though it delayed my move to law school, I'm glad I did it. My experience in the corporate world and my business education really help me, as a lawyer, think more strategically for my clients. As a result of my background, my natural tendency is to keep the focus on: What's the business goal, and what are you trying to accomplish? With that answer in mind, we can address the client's business goals and address the risks that may be necessary to achieve those goals.

CN: *Did you have an area of law in mind that you wanted to practice?*
SJ: My practice is quite diverse, but it's focused on technology. I spent many years as a trial lawyer, and I still actively litigate disputes that relate to software, technology or data. I also guide clients as they navigate privacy and security laws and regulations, and I help them develop policies to handle data and emerging technologies. Because of my background and experience, I am often appointed special master to the courts, and I serve as an arbitrator for the American Arbitration Association and the International Institute for Conflict Prevention and Resolution. Those roles have also led to recent designations as Fellow of the Chartered Institute of Arbitrators and recognition by the Silicon Valley Arbitration & Mediation Center as one of the technology arbitrators and mediators on their "Tech List." I've also taken on leadership positions, such as my role as president of the International Technology Law Association, an organization with lawyers from more than 60 countries, and as a Team Lead for the Technology Industry Group at Duane Morris.

CN: *When and how did cybersecurity become a focus of your practice?*
SJ: It was a natural progression. Much of my practice is focused on the intersection between technology, data and law. Privacy

and security were obviously very hot topics, and with my technology background, it was an easy transition.

CN: *Most lawyers don't have an MBA, even if they would benefit from one. How much does a lawyer need to know about business?*
SJ: Our clients are in business to make money. Legal disputes take their attention away from their primary goal. My aim is to think about my clients' needs and how we can achieve their goals. To do that, you have to understand their business, understand their industry, understand their goals and what they're trying to accomplish. I think that's why alternative dispute resolution [ADR] is a key part of my practice. I always try to put myself in the shoes of my clients and think strategically about what the business is trying to accomplish. And seek creative ways to accomplish their goals. Because I spent 16 years in the corporate world, that approach comes second nature to me.

I always try to put myself in the shoes of my clients and think strategically about what the business is trying to accomplish.

CN: *What do you see as the top risks for companies and their lawyers in 2019?*
SJ: I can give you two broad examples. The first area is privacy. Many clients recently addressed their compliance with the EU's General Data Protection Regulation [GDPR] and are starting to address the new California Consumer Privacy Act [CCPA], which comes into effect in 2020. CCPA is akin to a mini GDPR and will require certain clients to make significant changes in the way they handle personal information. Several other states recently introduced new privacy legislation, and the end result could be that businesses will have to navigate a broad array of varying state privacy laws. As a result of recent high-profile data breaches and the enactment of CCPA, momentum has been building for a national privacy law that would better protect individuals' personal information and pre-empt conflicting state privacy laws. The question is whether new federal legislation will be adopted before businesses are forced to navigate these emerging state laws.

CN: *And the second big one?*
SJ: Information security, which goes hand in hand with privacy, is where I see significant developments in the coming years. As we approach 2020 and 5G, the internet of things (IoT) and artificial intelligence (AI) will be more commonplace. When it arrives, 5G will be up to 1,000 times faster than 4G and will be the backbone for IoT and a truly connected world. The growing IoT world will produce an extraordinary amount of data, and AI will be used to identify patterns of data and take the next step toward connected intelligence. What that means for our clients is that not only will we see a rise of big data as we have never seen before, we will see significant security risks as we move forward into this brave new world. In a connected world, the stakes of a cyberattack are heightened. The impact of what would be an innocuous attack on one component could ripple down the line and create catastrophic damage. So all you really need is one minor vulnerability in one connected device to be exploited, and all of a sudden you have a risk to the whole chain. With connected devices in the workplace, in hospitals and in automated cars on the road, the risks are incalculable.

There are also many smaller companies developing their own connected devices or sensors, and they don't have the resources to engage in the same level of R&D as bigger companies to address every security concern and adopt a broad and fully vetted security solution. Without end-to-end security solutions, the weakest link is going to determine the overall security level of the chain of connected devices. We have already seen incidents where default security credentials have been hard-coded into the system, and those default codes are easily hacked—as evidenced by past breaches of security cameras, baby monitors and smart TVs. These are very significant issues that are going to have to be addressed. California has already passed a law that goes into effect in January 2020 requiring manufacturers of devices that connect directly or indirectly to the internet to have certain security features and to address default settings. These are really big issues, given that the scope of personal data collected is likely to be immense.

CN: *When your clients bring you in to talk about breaches, are there sometimes issues you're working through with them about cooperating with law enforcement and/or communicating with regulators about these breaches, and are there sometimes conflicting or ambivalent feelings about the wisdom of doing so?*
SJ: Particularly with respect to breaches, there are a large number of state breach notification laws that require notice to state attorney generals. Of course, businesses would want outside counsel to facilitate those discussions and respond to questions and requests for information.

CN: *But there are also the FBI, the U.S. Attorney's Office, and the Secret Service, and they encourage companies to share information with them. Sometimes they're the ones who actually tell the company, "Oh, you've been breached."*
SJ: That's very true.

CN: *How about that? How about dealing with law enforcement who are often eager to find out all they can? And often companies are wary about coming forward and are not sure if that's going to put them under the gun.*
SJ: That obviously is a concern for every client, because no one wants to have law enforcement peeking over their shoulder. Businesses should have experienced outside counsel engaged at the first inkling of a breach or when risk assessments are performed. Outside counsel should engage consultants and be the point person for discussion with law enforcement and state AGs. Outside counsel should act as the interface, so that they can be protective of the client as information is shared. At every step, it is important to be thinking about how to best protect the company now and if a future litigation or investigation should arise.

DuaneMorris

CN: *What are some of the concerns? Privilege is one, right?*
SJ: Privilege is extremely important, and yet it is often not considered by clients and their IT department when they are addressing information security, including such things as breaches or routine risk assessments. For example, businesses should regularly engage in an information security risk or vulnerability assessment to identify weaknesses and risks to the business. Unfortunately, these engagements are often handled exclusively by the IT department, with no thought by the company that the resulting report will provide an exhaustive list of risks and exposures that should be promptly remedied by the company. To the extent that a company has a future security incident—which is likely—that report will most likely become the key exhibit to show that the company was advised of the identified risks, yet failed to promptly and fully remediate them. It is therefore always advisable for outside counsel to engage consultants as they seek to identify the root cause of a breach, and the company's role in the breach, or when a consultant is engaged in a risk or vulnerability assessment. Like any other risk to the company, problems with the company's actions or failure to act should be addressed under the cloak of privilege. In-house counsel's involvement is often not sufficient because of the dual role they play within the company.

In a connected world, the stakes of a cyberattack are heightened.

CN: *How do the pieces of your background fit together in your practice?*
SJ: My practice generally involves addressing clients' business needs in the technology space, which obviously is a multifaceted role. Because of my background, I can speak tech, business and law, helping clients navigate these three very different and sometimes conflicting areas. In court, I can help by explaining complex technology issues to the court or fact finder. In the end, my ultimate goal is to help clients navigate their legal obligations, anticipate what issues may arise and strategically address those risks and issues.

CN: *So in a sense you're saying that you are trilingual: You speak business, you speak tech, you speak legal. Do you find yourself translating very often for clients?*
SJ: Actually, yes. There have been a lot of instances in my mediation and special master role, as well as my role with clients, where I bridge the gap between the tech folks and the business and legal teams.

CN: *What do you see as the in-house lawyer's role in tackling these issues? And how do you, with your particular skills, help them?*
SJ: The in-house lawyers have a very big job in today's digital world. They have so many issues to address. Because of my understanding of the technology and the industry, as well as my business background, I often work hand in hand with the in-house lawyers to identify risks and strategies to protect the company.

CN: *Looking back, are there lessons you learned about building a career—and specifically a career dealing with cybersecurity—that young lawyers today could learn from?*
SJ: I would advise young lawyers that they need to learn as much as they can about this area of law by reading, talking to people and staying up-to-date on new developments. They should also align themselves with organizations that have an interest in the area, volunteer and seek appropriate leadership positions. The goal is to obtain the full breadth of information on the topic and start to think like a lawyer about these complex and constantly changing issues.