OF COUNSEL
The Legal Practice and Management Report

ASPEN PUBLISHERS

Vol. 31 • No. 2 • February 2012

Leaking and Hacking . . .

Data Breaches Keep Privacy-&-Security Lawyers Increasingly Busy and Looking for Recruits

While some say that 2011 will go down as the year of the protestor, with demonstrators taking to the streets in the Arab Spring and Occupiers pitching tents from Wall Street to Main Street in the fall. Others look at last year and recall the devastation of the earthquake and tsunami in Japan, or the deaths of Bin Laden and Khadafy, or the confounded congressional gridlock, or the rise and fall of one fledgling GOP presidential candidate after another, or, heaven help us, they remember it as the year of Weiner's bulge.

But those in the business of cybercrime and protecting against cybercrime may think of 2011 as the year of the breach. Whether electronic information was intentionally hacked or unintentionally leaked, the world saw a plethora of data breaches. Some fairly big-name entities suffered massive penetrations last year, including Sony, Citigroup, Lockheed Martin, Epislon, Stanford Hospital, and even the International Monetary Fund, just to name a few.

What this means for consumers, investors, companies, and others, of course, is that private data ended up in the wrong hands, creating electronic-information nightmares and costing untold millions of dollars. What this means for lawyers practicing in the privacy and security area, and related fields, is that they've been busy. Very busy. They're working long hours to keep up to date on a river of new regulations flowing from Washington and state legislatures, advise clients on ways to prevent such e-spills, perform triage when breaches happen, and conduct a range of other activities.

"This is a hugely growing problem, in part because of the mass adoption of cloud data," says Gabriel Nugent, an attorney at Syracuse-based Hiscock & Barclay who says that half of his practice is white-collar criminal work, more and more of it in the cybercrime arena.

Certainly, the growth of in-cloud electronic storage is opening opportunities for hackers but breaches happen in many different kinds of systems, including those that probably ought to be put to rest and replaced. "It begins with information management and one of the biggest threats is the data that you're not managing well, which often turns out to be legacy systems that are still vulnerable to penetration," says Gordon Calhoun, a partner at Los Angeles's Lewis Brisbois Bisgaard & Smith, who works in many areas, including the data privacy and breach sector.

Because of the proliferation of breaches, state and federal legislators and various regulatory agencies have been scrambling to create a legal framework to help prevent privacy violations and compliance guidelines to follow after a breach has occurred. Clearly, it's not easy keeping pace with the volume and nuances of these laws and rules, and clients are depending on their lawyers to stay abreast of statutory changes.

"We now have 47 states with data breach statutes, with similar but not exactly the same rules, and we have to stay informed on what they are and help clients understand what their legal obligations are," says Holly Towle, a partner in the Seattle office of Pittsburgh's K&L Gates, whose practice includes work in

privacy and data security and electronic business issues. "To a large degree, that's why we stay so busy."

In the next several months legislative activity is likely to increase even more, requiring lawyers to examine the regulations' potential impact on their clients, according to Colin Zick, a partner at Boston's Foley Hoag, where he co-chairs the firm's security and privacy practice. "There's a lot of keeping up that you have to do," he says. "What we're seeing in 2012 is more legislation and more federal and state enforcement. And, we'll see a lot more of that."

Prevention and Reaction

At Foley Hoag, Zick and his team realize that clients' budgets are tight and try to adjust their legal approach accordingly. "We understand that very few clients can afford a 50-state compliance strategy," he says. "So we look for the states that have the highest, most sophisticated level of enforcement across the statutes, and try to generalize based on those as to what seems like a good level of action to take. California and Massachusetts, for example, tend to be leaders in the area. We may not pick up every little detail of other states, but we can do fairly well in getting close to compliance with this strategy."

Essentially, lawyers in this arena—and that covers a lot of different areas, such as transactional, IP, labor and employment, health care, and others—help clients in two ways: in the preventive and in the reactive scenarios, if you will. That is, they strongly encourage companies to use prophylactic measures and help them develop procedures and policies to prevent information leaks or hacks and set up protocols to follow in the event of a breach.

"More and more, companies are showing enough foresight to set up ways to prevent breaches and to recognize a key part of managing the breach exposure is preparation," says Calhoun, who adds that about 15 to 20 Lewis Brisbois attorneys work significant hours in this sector.

Once a breach occurs and is detected—and that sometimes takes awhile—companies need their lawyers to react quickly and thoroughly, which means attorney groups must be well-organized and ready to assess the situation and control the damage. "When a client calls with a data breach, the first thing to do is to think about mitigation," Zick says. "How do we keep this from getting any worse? We need to find out what exactly happened. What's the scope of the breach, how many individuals are affected, and what can we do to make sure that as little harm as possible is done to the affected individuals?"

Towle agrees and notes that often lawyers from other practice groups are called in to exercise their particular expertise with both precision and care. She explains: "When a client contacts us after a data breach, the first thing that we do is help them stop the bleeding. We have what I call the Internet safety group, a team that on an emergency basis can go in and help clients while they wait to get the real forensic experts. But whoever goes in has to be careful not to mess up the crime scene, so to speak."

Prompt Notification Is Key

At Denver's Holland & Hart, teams of attorneys also work in tandem. Matthew Cavarra is an H&H attorney who does mostly IP transactional work but is increasingly helping clients avoid breaches. "I do a lot more on the upfront protective side," he says. "As we do outsourcing transactions, we make sure that we're focused on all the protections you would expect regarding data security. We have a cross-practice here that is more reactionary. When there has been a security breach, our team brings in some of our white-collar defense attorneys to make sure that we're buttoned up and doing all the right responses."

Most likely, those responses include notifying the people whose privacy has been invaded, often the company's customers, which is usually required by law; failure to do this relatively quickly can ruin a company or at least cost it significantly.

"If you look at those data breach scenarios where significant fines have been imposed, usually there was a delay in notifying," Zick says. "The breach just got bigger because nobody took affirmative action to halt it. Individuals were left exposed because they didn't know that there had been a breach. Those are the sorts of things that make customers angry."

Naturally, if the client is a fairly well-known company, or even if it's not and the breach is extensive enough, the media will pick up on it. Lawyers can help control negative publicity and protect the company's brand, sometimes with the help of a public relations firm.

"This is going to be in the newspaper, if it's big enough," Zick says. "What are people going to say about you? Will they say that you responded well? Or will they say that you responded poorly? Those sorts of responses can either make or break a company. So it's important to be proactive and get out in front. Depending on the situation, we sometimes work with a PR firm. It has to be a coordinated approach."

Talent Is Thin

Clearly, this is work that's heating up quickly, and firms are having trouble finding attorneys with the right skill set to keep up with the increasing demand. "It's hard to recruit attorneys to do this because it's all so new," says Towle, who's book *The Law of Electronic Commercial Transactions* has three long chapters on data breaches and related topics. "You'd think, 'Well heck, privacy has been around forever.' But this is different. At law schools they need to find someone to teach this, and that's not easy. So we don't have enough generations yet. Mostly you have practicing attorneys who learned the area on the job, so you try to lateral in somebody, but it's hard to get somebody just out of law school. We have to train young associates."

That doesn't mean smart young attorneys aren't beginning to see this as a growth area. They are, but there just aren't enough of them with the expertise to contribute to the extent that many law firms need them to. "A lot of first-year and second-year associates are eager to get into the space," Cavarra says. "They see a lot of opportunity, but the nature of the projects doesn't always allow them to be heavily staffed with associates. We are in growth mode and we're looking; it's a pretty exhaustive search to find the right candidates."

Zick advises law students and young lawyers to explore the electronic privacy and security sector as one of at least a couple different skill sets in their career tool boxes; he has a health care background.

"I think that this is certainly a growing area that young attorneys should look at," Zick says. "There aren't a lot of people who are practicing exclusively in this area. Increasingly, they're going to be people who can carve out niches in this space or a combined niche of data privacy and consumer protection or something like that. It fits nicely with a commercial litigation background. It can also work with a health or an IP background." ■

—Steven T. Taylor