BUFFALO
BUSINESS FIRST

HOW I...

Combat cyber attacks

EVEN HODGSON RUSS ATTORNEY HAS BEEN A VICTIM OF HACKING

A few weeks ago, someone gained access to Gary Schober's credit card information and charged $300 for cigars in Tennessee. Schober, an asthmatic who doesn't smoke, was in New York at the time of the charge.

The story shouldn't come as too much of a shock: It's an increasingly familiar story, with incidents of credit card fraud and cyber hacking on the rise. Perpetrators gain access to information through large-scale breaches of data from companies such as Target and Home Depot, as well as personal information through health insurance companies.

What makes the incident involving Schober notable is his job as a cyber law expert at Hodgson Russ LLP, where he focuses on helping companies learn how best to prepare for and react to cyber fraud. No one is really safe, he said.

"Each of us as individuals needs to be sensitive to the protection of our information because hackers are just as likely to go after an individual's information as they are a Fortune 500 company," he said. "Obviously, what they're looking for is different and what they'll do with the information is different, but there are hackers that work in every segment of the population."

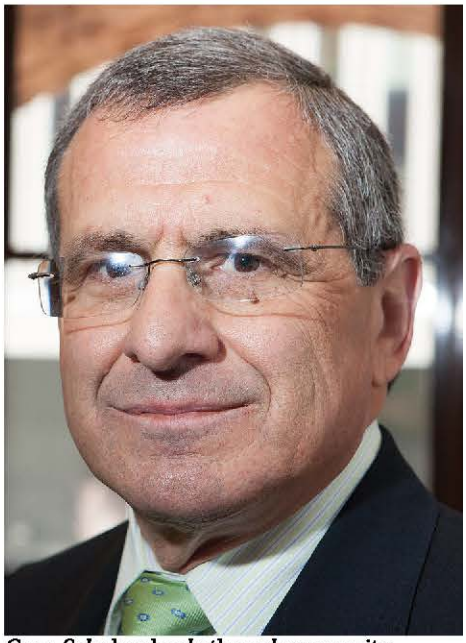
Schober came to Hodgson Russ in 1979 with a background in business law and an undergraduate degree in math and computer science. Back then, that meant punch cards and coding, but it gave him a base of knowledge for the personal computer age. He has reinvented himself along the way to help clients in Western New York and in the firm's New York City office.

What kind of work do you do for clients? First, you get the clients who have suffered a security breach, the after-the-fact. And obviously their situation is very different from the people who come to us and ask for preventative measures to help avoid problems. The people who have already suffered a breach are very motivated to address it as quickly as they can. On the other side of the equation, you could get a client who sends an email to the wrong person. That can be a very quick fix.

How about preventive measures? Security audits are becoming commonplace today, either because clients are deciding they need or want one, or because someone is putting pressure on them to have one done – often a client or customer. They usually begin with a questionnaire, where the person performing the audit will ask questions about what you do and how you do it. They'll come in and interview staff or do an on-site inspection of systems. Sometimes they'll sit at an idle station and see what they can do as an outsider with penetration testing and ethical hacking. Then there's the legal analysis, where we'll look at what the client does and try to identify all the laws applicable to what they do.

Are there any companies where cyber security is not an issue? I don't think so. If nothing else, every company will usually have some human resources information, and that by its very nature is personal and they have a need to protect it. I think the need to be worried about hackers is across the board. The amount of time, energy and resources you need to devote to it will vary whether you're a very large company with highly sensitive information or just running a delicatessen.

What kind of change will that mean for a company? Process is a big part of this. You do have to change the way you do business. When we did a security audit here, we got a very nice report with a long list of suggestions. One of the suggestions was that all the lawyers should have locks on their doors, because we all have sensitive papers we put on our desks and at night we go home. We concluded that culturally that would be a huge mistake. It wouldn't be good for our business because we encourage lawyers to talk to each other and we want an open-door policy. Whatever you do, you have to be consistent with your firm's culture. Security is important; I spend a lot of time doing it and helping people. But it can't drive everything. There's a fair bit of trial and error here, but you have to keep in mind that the goal is always to reduce risk. You're never going to remove risk. That's just impossible in today's environment.



Gary Schober leads the cyber security practice at Hodgson Russ LLP.

– Tracey Drury

GARY SCHOBER

Employer: Hodgson Russ LLP

Title: Practice leader of emerging companies and venture capital; and privacy, data security and cyber liability. Former president/CEO, 2005-12

Year joined firm: 1979

Education: J.D., Georgetown University School of Law

Hometown: Seaford, Long Island