Long Island BusinessNEWS

FEB. 14-20, 2014 | VOL. 61 | NO. 7 | $2.00 | libn.com

Targeting data breaches

Cybersecurity issues offer growing opportunities for law firms, IT providers

By BERNADETTE STARZEE

Recent data breaches at Target and Neiman Marcus have spotlighted technology security issues, making it easier for one Long Island law firm to spread the word about its new cybersecurity practice group.

"The media is doing a great job of marketing" the importance of safeguarding sensitive data, said Steven Rubin, partner and co-chairman of the new cybersecurity practice group at Garden City-based Moritt Hock & Hamroff, noting every new Google search he does seems to bring news of another breach.

Moritt Hock, which officially launched the practice group Jan. 1, began preparing for the launch in mid-2013.

"Cybersecurity is an exciting, growing area," Rubin said. "There's not a lot of experience in it anywhere – the laws are young, and there's a hodgepodge of laws trying to cover all the related issues."

The firm took an interdisciplinary approach in establishing the cybersecurity group, culling seven attorneys from various practice areas. Rubin, who heads the firm's patent practice, has a technical background, while the other co-chairman, A. Jonathan Trafimow, chairs the employment law practice. The other attorneys have expertise in healthcare, marketing, criminal law, corporate, securities and electronic litigation.

Rubin expects much of the group's work will be preventive in nature.

"Companies will want to have some cybersecurity policy in place based on the level of the sensitivity of the data," he said. "We can help clients identify risk and set up preventive systems, and figure out what to do if there is a breach and what notification would look like."

Another projected growth area is in the compliance arena, he added.

Cybersecurity issues affect any company that uses email or the Internet to communicate and conduct business.

"Every business today is an e-business – every company has exposures," said Shari Claire Lewis, a partner in the product liability and toxic tort, professional liability and intellectual property practice groups at Rivkin Radler in Uniondale.

STEVEN RUBIN: His firm launched a cybersecurity practice to meet increasing need.

Companies that collect private information – such as driver's license IDs, Social Security numbers, personal health information and financial information – must be particularly vigilant about safeguarding their processes, said Giuseppe Franzella, a litigation associate at Lazer, Aptheker, Rosella & Yedid in Melville.

"They may have to pay real damages if the information falls into the wrong hands and people have their identities stolen," he said.

As technology and the cloud become more prevalent, there are more questions about who's responsible for security, said E. Christopher Murray, chairman of the Nassau County Bar Association technology and practice management committee, which hosted a cybersecurity seminar for attorneys last month that was very well-attended.

While some firms, like Moritt Hock, are setting up distinct practices to meet increasing demand, others are expanding cybersecurity services within an existing practice group, Murray said.

"It dovetails into a general intellectual property practice, so it may become part of that," he said.

Lewis, who describes her practice as being at the "intersection of law and technology," has collaborated with about 10 Rivkin Radler attorneys with diverse concentrations on various cybersecurity matters, including response to data breaches.

New York is one of 46 states with security breach notification statutes in place.

"What's missing is a federal statute that would tell companies large and small that if they have a data breach, this is what they have to do and when to do it," Lewis said.

Individuals or entities doing business in New York that experience a breach must expeditiously notify affected parties in addition to the state Attorney General, the Division of State Police and the Department of State's Divisions of Consumer Protection, according to Franzella.

Data breach response should also include steps to restore reputation – such as offering affected parties free credit monitoring services, as Target and Neiman-Marcus have done – as well as finding the source of the breach and plugging it, Lewis said.

"Data beaches must be addressed jointly with legal and IT," she said. "A trusted IT professional has to be at the table and will have information that a law firm is not going to have."

Perhaps no industry has greater exposure to the threat of data breaches than healthcare. New HIPAA privacy and security rules introduced last September call for greater penalties for HIPAA-covered entities that fail to update their policies and procedures or conduct a risk analysis on their technology systems. The new laws also expand compliance requirements beyond the hospitals, doctors' offices and health insurance providers that directly handle protected health information to bestow equal responsibility on business associates – any organization or person working in association with or providing services to a HIPAA-covered entity.

Flexible Business Systems, a Hauppauge-based IT provider with a healthcare practice, officially launched its HIPAA Helpers division last month to help clients comply with the new rules.

"The document is 563 pages, and most clients are confused about what they need to do," said Kevin Edwards, director of healthcare services for the company, whose HIPAA services include risk analyses of IT infrastructure, policy and procedure manuals, staff training and audit support. "The new laws have put a greater emphasis on the security side."