THE STANDARD
NEW ENGLAND'S INSURANCE WEEKLY
Published Since 1865 Boston, Mass.
November 28, 2014 Vol. 275 No. 17

Proactive Safeguards Can Reduce Risk of Cyber Fraud, Liability

Cyber Expert Speaks at SSIIA Meeting

BRAINTREE, MASS. — Attorney Brendan J. Gaughan of Boston's Governo Law Firm spoke to the South Shore Independent Insurance Agents (SSIIA) at their November meeting about the importance of being prepared for the inevitability of cyber attack. He pointed out that while the insurance industry has taken steps to promote data security and financial protection over the past few years, it will always have a certain degree of vulnerability to cyber breaches. Compounding this troubling situation, Gaughan continued, is that insurance agencies are additionally "subject to a myriad of data security laws" with which they must be in compliance.

Insurance agencies routinely collect vast amounts of personal information and are "constantly under malicious cyber attacks," Gaughan stated. As a result, experiencing some sort of data security breach is unavoidable. "The hackers are always going to be one step ahead of you," he cautioned. "It's really not a matter of *if* your company's computer system is going to be hacked or *if* the personal information that you collect on a regular basis is going to be compromised … it's really a matter of *when*."

Despite heightened awareness of data security and cyber liability issues, insurance agencies of all sizes are susceptible to cyber attack. Gaughan referenced a recent Wall Street Journal report indicating that 40% of the major insurance companies in the United States experienced cyber breaches last year.

As a means to counter or at least reduce cyber risk and liability, Gaughan strongly recommended that agencies have certain measures and controls in place as safeguards. The repercussions of data breaches can be very costly for insurance agencies, he warned, especially for a small agency, which could go out of business.

The definition of personal information is also "an evolving, expanding concept," according to Gaughan, and it is important for insurance agencies to be aware of what this entails. "You need to have a meaningful understanding of what the laws require in order to protect this information," he stressed, citing Massachusetts data security laws mandating that such information be encrypted once collected by an agency.

Massachusetts' security compliance laws further require all organizations collecting personal data to have in place a written information security program (WISP). Such a plan must contain the "evaluation of reasonably foreseeable risks to private information; employee training; policies and procedures for storage, access and transport and documentation of responses to a security breach."

Gaughan advised that an agency's WISP be developed in tandem by an attorney, who would provide legal guidance for what the agency needs to have in place, and IT personnel, who would have the technological expertise to implement the plan.

In terms of data breach notification, he emphasized it must be done "expediently and without unreasonable delay."

There are various ways to reduce risk, such as ensuring vendor compliance with data security guidelines (including having a written contract in place with them to avoid agency liability), effective employee training and regularly revisiting and updating policies and procedures as needed.

"Don't gamble with data security — take action now," Gaughan advised. ■