New England Real Estate Journal
nerej
THE LARGEST COMMERCIAL/INVESTMENT REAL ESTATE NEWSPAPER IN THE WORLD
Reprint | nerej.com | Friday, April 15, 2016

Connecticut municipalities to follow data breach laws

Burt Cohen

Murtha Cullina LLP

Daniel Kagan

Murtha Cullina LLP

In the world of data breaches, John Chambers, CEO at Cisco, explained it best: "There are only two kinds of companies. Those that were hacked and those that don't yet know they were hacked." With the ever increasing rate of data breaches nationwide, and with no industry left unscathed, Connecticut enacted Public Act 15-142, "An Act Improving Data Security and Agency Effectiveness." This Act's passage creates an opportunity to revisit Connecticut's data security and breach notification statute to analyze the extent of its reach. Besides applying to Connecticut businesses, the statute also applies to municipalities, as described in further detail below. And, not unlike the private sector, municipalities are just as susceptible to the ongoing threat of data breaches. The best practice for municipal government is to adopt and implement a written information security plan (WISP), tailored to the specifics of Connecticut town government, which establishes procedures to protect confidential data from disclosure. Recent events continue to show, municipalities are the targets of hackers. Two events in particular provide ripe examples of how municipal and state governments are at risk for various types of data breaches. Earlier this month the town of Medfield, Mass. was the target of a ransomware attack. The attack locked its computer system for almost one week before the town paid the requested ransom. And, in a more "typical" data breach event, 14,200 people, mostly current and former Salt Lake County, Utah employees had their personal information exposed in a data breach last summer. This data breach was confirmed after the Utah attorney general recently completed an investigation. In this age of instant information, municipalities have all types of information that would be considered "personal information" under Conn. Gen. Stat. § 36a-701b. The statute defines "personal information" to include "an individual's first name or first initial and last name in combination of one, or more, of the following data: (A) Social Security number; (B) driver's license number or state identification card number; or (C) account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account." While this definition of personal information does not include any publicly available information that is lawfully made available to the general public from federal, state or local government records or from widely distributed media, Conn. municipalities now accept payments via credit or debit cards for taxes and fees, along with the usual personnel information for municipal employees and officials. Further, under this statute, "any person who conducts business in this state, and who, in the ordinary course of such person's business, owns, licenses or maintains computerized data that includes personal information" is subject to the statute's data security and breach notification requirements. The key question arising from the Conn. data breach law is whether a municipality constitutes a "person who conducts business in this state." As it turns out, under the applicable definitional statute, Conn. Gen. Stat. § 36a-2, "person" is broadly defined to include not only companies, but also any municipal government or agency. Thus, Conn. municipal governments need to secure the types of personal information they own, license and maintain.

Burt Cohen is a partner and Daniel Kagan is an associate with Murtha Cullina LLP, New Haven, Conn.