nerej
CELEBRATING 55 YEARS

Cyber and data protection - real problems for real estate professionals

October 02, 2014 - Spotlights

Hardly a week goes by without some report of a major hacking incident or security threat to some large corporation or government entity. We shrug it off as a concern only for the "big guys". What cyber thief would be interested in us? The answer is - the great majority of them. While privacy or data breaches to small business don't always make the news, they occur with frightening regularity.

Consider the real estate agent, mortgage broker or attorney, whose professional duties rely on the accumulation, dissemination and storage of someone's most intimate information. Credit applications, rental and purchase and sales agreements and closing documents may contain social security numbers, driver's license number, bank account information and more. Most of this information is kept on a laptop, cell phone or tablet. Real estate professionals are extremely dependent upon their electronic devices. A 2010 study by a national privacy group found that almost 50% of all stolen laptops had confidential data on them, with a high percentage of that being unencrypted. Has anyone ever done a study on cell phones left in bars, restaurants or restrooms? What about your professional networks? One study showed 7 out of 10 mortgage companies share data across state lines, with each state having their own privacy laws and requirements. Further, a 2010 NAR study found that 80% of member respondents did not know about their state's privacy laws, and more than 50% had no data protection protocol for their firms.

Examples of Privacy/Date Breaches

* In March 2012, a Massachusetts property manager was fined $15,000 by the state for a stolen laptop with unencrypted data. Additional financial burdens would include notifications and potential liability suits
* Cyber criminals hacked data from rental listings and collected the deposits and rents
* A large real estate firm was fined, and sued, for dumping documents in a dumpster, later stolen and used to gain personal information about clients

What Is the Cost?

Should a data breach occur, all states require that the affected parties be notified. In 2011, the average cost of each notification was $194. The average cost of replacing a stolen laptop was almost $50,000. That cost, which could be considerably higher, would need to contemplate the cost of notifications, forensic work to find the source of the hack, civil penalties and third party liabilities. Hidden costs include loss of productivity and consumer trust.

Massachusetts Privacy law sets a civil penalty of up to $5,000 for each (one consumer file) violation, and $50,000 for each improper record disposal. Many states require written privacy procedures, compliance officers and more.

What Can You Do?

There are ways to protect against a breach. NAR offers a "Data Security and Privacy Tool Kit". Tufts

University offers a "Guide to Massachusetts Data Privacy Law" and many other resources exist.

Cyber/privacy insurance is now available and affordable for small businesses. Such insurance may cover expenses for civil penalties, notifications, liability and handle the myriad laws and requirements of each different state. It will provide coverage for data breach, hacking, dumpster diving, viruses, identity theft and more.

The threat to our data is real. Your clients, and the law, demand that you respond.

John Torvi is vice president of marketing & sales for Herbert H. Landy Insurance Agency, Needham, Mass.