QUADRANT INSURANCE MANAGERS

COMPASS REPORT

January 2012

Topic: Data Breaches

Many of our agents have been asking us very good questions about cyber liability, so we thought it might be helpful to send some current information that we hope will be useful. And of course, we are available to respond to any of your questions that may arise.

I came across a current cyber article that I thought I would share with you. Did you know that **hack attacks are now the leading cause of data breaches?**

According to an article in InformationWeek, an upcoming study from the Identity Theft Resource Center (ITRC), which assessed all known information relating to the 419 breaches that were publicly disclosed in the United States in 2011, **hacking, followed by data lost in transit and insider attacks, were the leading data breach culprits in 2011.**

- Last year, data breaches triggered by hacking, including card-skimming attacks--were at an all-time high, and responsible for 26% of all known data breach incidents. The next leading cause of breaches was data on the move (18%)--meaning electronic storage devices, laptops, or paper reports that were lost in transit--followed by insider theft (13%).
- Malicious attacks accounted for 40% of publicly disclosed breaches, while 20% of breaches were the result of accidental data exposure.
- Data breach incidence varies by industry. In 2011, the government and armed services saw the greatest volume of records exposed (comprising 44% of all exposed records), followed by non-financial businesses (33%), medical and healthcare groups (16%), educational institutions (4%), and banking, credit and financial firms (3%).
- Non-financial businesses, as well as medical and healthcare groups, saw the largest incidence of insider theft, while non-financial businesses were hacked far more often than other industries. Notably, 17% of all breaches involved hack attacks against businesses, compared with hack attacks against banking, credit and finance (3%), education (2%), medical and healthcare (2%), and government and military (1%).

By Mathew J. Schwartz
InformationWeek
January 12, 2012

Link to read the complete article:
http://informationweek.com/news/security/attacks/232

Karen Harris

Quadrant Insurance Managers
614.841.1425 / Ext. 121
www.quadrant-us.com

Cyber Markets (alpha order)

- Arch Specialty
- AWAC (Darwin)
- Beazley
- Chartis
- Erisk (Scottsdale)
- Ironshore
- Lloyds
- Markel
- RSUI
- RLI
- ThinkRisk
- Torus

Our markets are AM Best Rated "A-" or higher

Quadrant Recent Industry Classes:

- Education
- Healthcare
- Technology
- Insurance Agency
- Not for Profit
- Retail

Please contact me with submissions and questions about cyber liability for your insureds and your agency.

Thank you!

Recent Data Breach Incidents

December 2011 Good News Garage
14,000 potential records

A home burglary resulted in the loss of an encrypted data tape. The tape was inside a backpack that was stolen from an employee's locked car while it was parked at home. The data tape had names, addresses, and in some cases Social Security numbers of Good News Garage donors dating back 15 years.

December 2011 Restaurant Depot, Jetro Cash & Carry
300,000 potential records

People who shopped at Jetro or Restaurant Depot between September 21 and November 18 may have had their credit or debit card information taken by a hacker. Customer names, card numbers, expiration dates, and verification codes were exposed. The breach investigation began when the parent company became aware of customers experiencing card fraud.

December 2011 Extreme Pizza
Unknown potential records

Someone hacked into the Extreme Pizza computer system and took information from cards that had been swiped by Extreme Pizza. The thefts date back to September of 2011. Credit card transactions were moved to a different type of card reader in response to the breach.

December 2011 data breaches — **Privacy Rights Clearinghouse**