



# :/RISK/=

## CYBER RISK INSURANCE

*-Josh Bindl, Director of Programs and Services, Wisconsin Counties Association*

**W**e live in a world where endless amounts of data are stored electronically. Any entity who has a website or stores personal identifiable information can be vulnerable to a data breach. In a 2011 study, Verizon reported that 3 out of every 4 data breaches go undetected for weeks or longer. As each day goes by, the cost of most breaches escalates. This allows the data thieves a head start in using the compromised information to their benefit.

Local governments hold sensitive records, such as employee records; payment records for taxes, fines and fees; inmate records; and information on individuals receiving government assistance to name a few. In addition, employees have access to both internal and external databases filled with information about the general public. All of this information exposes local government to liability should a data breach occur.

Many policies and procedures can be put in place to reduce this risk. Requirements on the usage of data encryption, as well as authentication methods, such as password protection are just some of the tools that could be implemented immediately to reduce the risk of a data breach.

Close to half of all breaches are due to employee error or negligence. These acts can occur without malicious intentions on the part of the employee. Training on best practices for storing data, sharing files and transporting hardware helps employees better protect data, as well as the public they are entrusted to keep secure.

While a number of safeguards exist to help prevent a cyber attack, even the best controls are no match for human error. In December, the Wisconsin County Mutual Insurance Corporation (County Mutual) Board of

Directors took the necessary steps to add cyber coverage to its liability policy covering its 52 member counties. This policy includes coverage not only for the cost and defense of a claim made in relation to a security breach, wrongful acts of website publishing by the covered entity and computer fraud, but also for the cost of public relations efforts to protect or restore the reputation of the covered entity, notification to those impacted by the act, and post-event call-in centers and credit monitoring for the victims of a breach.

Budgets are difficult across all levels of government. Although the cost associated with a cyber breach can reach extraordinary levels, budgeting for such an unlikely event may not be prudent. A more cost effective alternative is financing this exposure through the purchase of a cyber risk policy.

The good news for the 52 counties who are already members of the County Mutual is that they already have cyber risk coverage by paying their 2014 premium. This coverage will be effective February 1, 2014 for members. The continued success of County Mutual in reducing claim frequency and severity has allowed for cyber risk coverage to be purchased without any increase in premium.

Members of the County Mutual will be receiving the covering endorsement, a brief coverage explanation and an introduction into the risk management training that will be offered through the remainder of 2014.

There is no doubt that Target's corporate leadership believed the necessary steps were taken to prevent the recent and widely publicized data breach. If your county does not have coverage for cyber risk, consider what exposures the county faces. 