CTSI
Serving Colorado's Counties

Technical Update

Volume 20 Number 3 April 11, 2016

Cyber Risk: Public Sector Continues to Encounter Risk

As dependence on technology increases, the greater the increase of exposure to cyber risk and security breaches. Ensuring customers' privacy and confidentiality means finding ways of offering secure payments and protecting private information at every point in the operational process.

Foreign hackers have breached critical infrastructure of federal agencies 150 times over the past four years, specifically targeting the United States. The U.S. Department of Homeland Security announced a 20% increase in the number of cyber incidents being handled by its response team at the end of its fiscal year in September 2015.

Small and mid-sized businesses (SMEs) are faced with the decision whether or not to purchase cyber insurance coverage. An industry survey by the Council on Insurance Agents & Brokers (Hoffman, 2015) showed a 24% increase in take-up rates by larger companies while SMEs are lagging. There are conflicting opinions regarding the future cost of cyber coverage. Over 50% of survey respondents reported that pricing was flat, 28% said it has increased, and 16% said it has decreased. For 2016, CAPP had no rate change. An industry survey by Insurance Day and law firm Weighmans revealed that a large majority of respondents in the insurance industry predict an increase in price over the next 12 months.

What This Means for Counties

With the public sector's growing reliance on technology, hackers will continue to breach systems, and cyber risk will continue to be a business concern. Cyber insurance coverage and the cyber legal/regulatory landscape will also evolve. Insurance will eventually be a standard line of business for most insureds. CAPP members have coverage for cyber exposures through the pool and CTSI will continue to monitor coverage limits and rates.

For more information, contact CTSI at 303-861-0507.