NEW YEAR, NEW RISKS: CYBER ISSUES TO CONSIDER IN 2014
By Gary Sorenson, CEA, CLCS, PLCS, President,
Insurance Brokers of Minnesota, Inc.

The New Year represents a time for many companies to evaluate their successes, business goals, operations and risks. While businesses may not be able to anticipate every risk that they will face this year, one thing is for sure: cyber security should be a concern for businesses large and small. Undoubtedly, the cyber landscape is continuing to evolve as cyber criminals become smarter and more creative about their tactics to steal information from companies.

Technology and the sharing of information are central parts of both business operations and our everyday lives, which is why it is imperative that businesses understand the many forms cyber risks take, so that they can protect, their data, their bottom line, their customers and their reputations.

In fact, according to the Travelers' Consumer Risk Index, 64 percent of individuals cite personal privacy loss or identity theft as a significant concern. And, according to the Verizon 2013 Data Breach Report, there were more than 47,000 reported security incidents and 621 confirmed data breaches from the past year. Over the entire nine-year range of this study, that tally now exceeds 2,500 data breaches and 1.1 billion compromised records. And, those represent only reported incidents

So, what should businesses be concerned about when it comes to cyber security in the New Year?

Protect Secure Customer Information. The greatest risk exposure is the loss of personal information. This can happen if an employee loses a laptop or when a hacker obtains sensitive personal information from the insured's computer system, which can include laptops, mobile devices, tablets, etc. As a result, a customer or number of customers may be able to bring claims against the insured for allowing access to their information.

Secure Passwords. Another common way for hackers to penetrate a company's system is through breach of passwords. Employees with relatively common passwords leave their computers and accounts open to attack. A best practice is to require employees to use more complicated passwords and to change passwords on a regular basis.

Extortion Events. Hackers also are getting more sophisticated, sometimes forming syndicates of like-minded criminals to share information and new techniques, including extortion events. Cyber extortion is a crime involving an attack or threat of attack against an organization, coupled with a demand for money to prevent or stop the attack.

While extortion is not new, the emergence of cyber extortionist has recently began to rise. Today, new malware and hackers are tapping into systems for financial gains and to create disruption. But, whether intentionally or not, if they gain access to personal information, a data breach occurs.

“Hactivism” Another one of the biggest eye-openers is so-called “hacktivism.” Hacktivism is the act of breaking into a computer system, for a politically or socially motivated purpose. There have been dozens of cases reported where commercial websites have been altered or disabled, sensitive information has been stolen and even government systems have been breached. This trend is interesting because the perpetrators are not doing it for monetary gain, but rather to raise awareness of an issue.

As more and more businesses are faced with these issues and risks, it is important to proactively protect against them. A great first step is talking to an independent agent at Insurance Brokers of MN, Inc. who can help educate them on their businesses’ cyber risk exposures.