

## Cyber Security 2 — HealthCare Providers Warned by FBI



We're halfway through 2014 and the U.S. has experienced 368 data breaches. The latest is the Montana the Department of Public Health and Human Services. It experienced a hacking a year ago that was just discovered. The attack affects 1.3 million people in a state with a population of just one-million.

More than 3,000 Montana employees saw their person information compromised. Their banking information was on the hacked servers.

The Identity Theft Resource Center is the source of the 368 number. It says 32.9% of those hacked were from the business community. And those same businesses account for 60% of the records taken in the 368 incidents.

As noted by the Montana Department of Public Health and Human Services, the health insurance industry is more vulnerable than the financial and retail sectors. That's why the FBI has issued a private industry notification (PIN) warning to healthcare providers to beef up their cyber security.

It seems that healthcare data has more value on the black market than other information. The reason is because they not only contain personal banking information and Social Security numbers, but they offer important prescription information.

The FBI told *Insurance Journal* that healthcare data can be sold for \$1,000 or more.

The PIN warning says "the healthcare industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely."

Another plus for hacking into healthcare providers is that it takes longer for the stolen information to get noticed.