BioSpectrum
the business of Bio & Health Sciences
ASIA EDITION

FBI: Healthcare industry has lax cyber protection

22 August 2014 | News | By BioSpectrum Bureau

Singapore: One of the leading hospital groups from the US came under a cyber attack emerging from China. The criminals are said to have stolen Social Security numbers and other personal data belonging to 4.5 million patients. This has resulted in a serious warning issued by the Federal Bureau of Investigation (FBI) to the healthcare industry and its lax data protection.

Reports quoted security experts as saying that the hacking group, known as 'APT 18,' may have links to the Chinese government. "APT 18" typically targets companies in the aerospace and defence, construction and engineering, technology, financial services and healthcare industry, said Mr Charles Carmakal, managing director with FireEye Inc's Mandiant forensics unit, which led the investigation of the attack on Community Health in April and June.

He said in a news report, "They have fairly advanced techniques for breaking into organizations as well as maintaining access for fairly long periods of times without getting detected."

In a regulatory filing, the company explained that the information stolen from Community Health included patient names, addresses, birth dates, telephone numbers and Social Security numbers of people who were referred or received services from doctors affiliated with the hospital group in the last five years.

The stolen data did not include medical or clinical information, credit card numbers, or any intellectual property such as data on medical device development, said Community Health, which has 206 hospitals in 29 states.

The attack is the largest of its type involving patient information since a US Department of Health and Human Services website started tracking such breaches in 2009. In a previous attack on a Montana Department of Public Health server about one million people were said to be affected.

Chinese hacking groups are known for seeking intellectual property, such as product design, or information that might be of use in business or political negotiations.

Another report explained that social security numbers and other personal data are typically stolen by cybercriminals to sell on underground exchanges for use by others in identity theft.

The FBI has issued a warning to the healthcare industry claiming that its protections were lax compared with other sectors, making it vulnerable to hackers looking for details that could be used to access bank accounts or obtain prescriptions.

In a flash alert reported by Reuters, the agency said, "The FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."

It added, "These actors have also been seen targeting multiple companies in the healthcare and medical device industry typically targeting valuable intellectual property, such as medical device and equipment development data."
Meanwhile, Community Health said that it has removed malicious software used by the attackers from its systems and completed other remediation steps. It is now notifying patients and regulatory agencies, as required by law. The company said it is insured against such losses and does not at this time expect a material adverse effect on financial results.