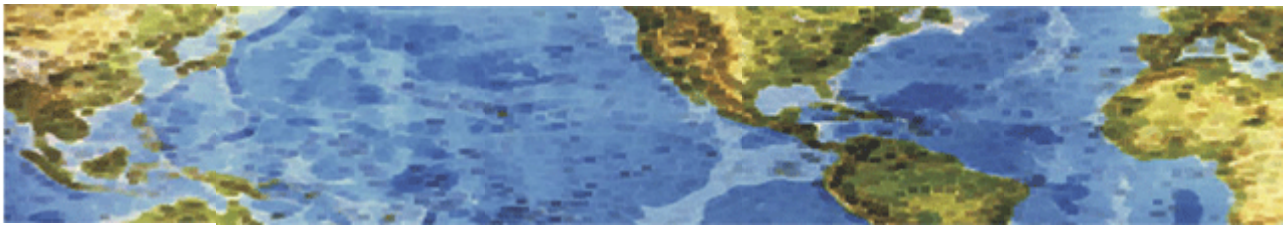
HALL ASSOCIATES



Risk-Based Decision Making Commentary
25 August 2014 Newsletter

Community Health Systems, which was the victim of a cyberattack, runs 206 hospitals in 29 states, including the Trinity Medical Center in Birmingham,

200 Hospitals Hit Affecting 4.5 Million Patients

Tennessee-based Community Health Systems (CHS) says that intruders accessed its system over a three-month period earlier this year, compromising patient names, addresses, and Social Security numbers (SSNs) of 4.5 million people. The company maintains that medical and financial information was not affected. The company, which operates 206 hospitals in 29 states, said in a filing with the Securities and Exchange Commission on Monday that that the attackers had bypassed its security systems and stolen data that also included birth dates and telephone numbers for the patients, who had been referred to or treated by doctors affiliated with the company over the last five years. The company is required to notify affected patients and agencies under the Health Insurance Portability and Accountability Act, which protects such personal data. The company claims that the attacks emanated from China. Information in CHS's Securities and Exchange Commission (SEC) Form 8-K filing says that the intruders were attempting to obtain medical equipment device development information, but were thwarted in their efforts.

http://www.darkreading.com/community-health-systems-breach-atypical-for-chinese-hackers/d/d-id/1298095?

4.5 million is smaller than 140 million (number of records stolen from E-Bay), but unwanted disclosure of personal medical information is the one area of information privacy that will draw widespread and continuing outrage from powerful people. The data taken in this attack isn't medical, **but the lack of effective cybersecurity in hospitals and their associated local doctor's offices** is well known by the black hat 'researchers' and cyber criminals.

Multiple medical institutions have paid lots to extortionists to keep their loss of data from being exposed; one health care information system was so full of holes that one researcher actually **had to build in security** before he could use it in a simulator. Too many hospitals and local doctor's offices and pharmacies still consider cybersecurity primarily a compliance issue and have not been forced to bake in security, nor have they invested in staff (or consultants) who have the skills to protect from, identify, and respond quickly to attacks. I wonder how many of our hospital, doctor's office and other medical practitioner systems have been breached and no one even knows how to find out, much less protect themselves.

HALL ASSOCIATES

Malicious software in cash registers could affect more than 1,000 US retailers, gov't warns

More than 1,000 U.S. retailers could be infected with malicious software lurking in their cash register computers, allowing hackers to steal customer financial data, the Homeland Security Department said Friday. The government urged businesses of all sizes to scan their point-of-sale systems for software known as "Backoff," discovered last October. It previously explained in detail how the software operates and how retailers could find and remove it.

Earlier this month, United Parcel Service said it found infected computers in 51 stores. UPS said it was not aware of any fraud that resulted from the infection but said hackers may have taken customers' names, addresses, email addresses and payment card information. The company apologized to customers and offered free identity protection and credit monitoring services to those who had shopped in those 51 stores.

Backoff was discovered in October 2013, but according to the Homeland Security Department **the software wasn't flagged by antivirus programs until this month**. The news was the latest development in an ongoing battle between retailers and hackers. Retail giant Target, based in Minneapolis, was targeted by hackers last year and disclosed in December that a data breach compromised 40 million credit and debit card accounts between Nov. 27 and Dec. 15. On Jan. 10, it said hackers stole personal information — including names, phone numbers and email and mailing addresses — from as many as 70 million customers.

Over the past year, the Secret Service has responded to network intrusions at numerous businesses that have been affected by the "Backoff" malware The malware has likely infected many victims who aren't aware that they have been compromised. Meanwhile, seven point-of-sale-system providers or vendors have confirmed that they have had multiple clients affected, the DHS said

Target, the third-largest retailer, has been overhauling its security department and systems in the wake of the pre-Christmas data breach, which hurt profits, sales and its reputation among shoppers worried about the security of their personal data. Target is now accelerating its $100 million plan to roll out chip-based credit card technology in all of its nearly 1,800 stores. So-called chip and pin technology would allow for more secure transactions than the magnetic strip cards that most Americans use now. The technology has already been adopted in Europe and elsewhere.

The Backoff program itself is not unique. Like other malware designed to steal financial information from retail customers, the software gains access to companies' computers through insufficiently protected remote access points and duping computers users to download malware. But its wide deployment by hackers and its repeated updates over the last six months make it a serious threat for consumers and business.

http://www.foxnews.com/tech/2014/08/22/malicious-software-in-cash-registers-could-affect-more-than-1000-us-retailers/?intcmp=obnetwork

http://online.wsj.com/articles/more-than-1-000-businesses-affected-by-backoff-http://online.wsj.com/articles/more-than-1-000-businesses-affected-by-backoff-malware-1408746408malware-1408746408