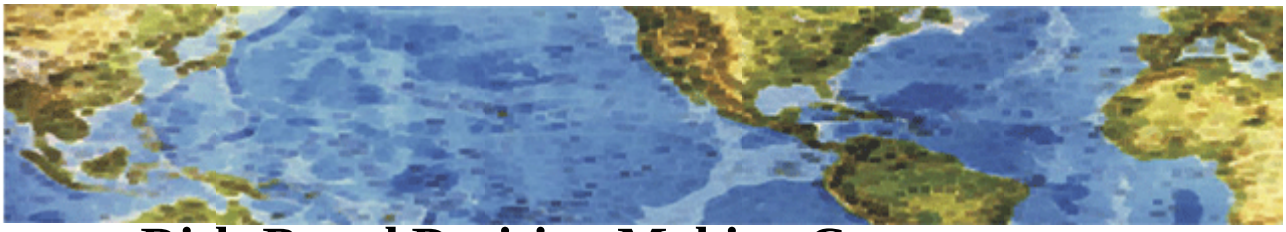
HALL ASSOCIATES



Risk-Based Decision Making Commentary
27 July 2014 Newsletter

No slowdown this summer on the cyber risk & data breach front.

I thought a sampling of the mid-July articles on cybersecurity problems and data breaches might be interesting. These types of risks and breaches happen all the time and are increasing every month. Determining your vulnerabilities and preparing for compromise of your personal and business data does seem to be getting more urgent every day. If you would like to learn more about any one article and see many more such notes, go to the URL noted at the end of this newsletter or simply google the title. I get a report on different ones like these at least once a week.

DMHC, Blue Shield Announce Data Breach Affecting 18K Calif. Doctors

The Social Security numbers of about 18,000 California physicians were accidentally released with other data by Blue Shield of California and the state Department of Managed Health Care, Medical Daily reports.

Stolen Laptop Leads to Data Breach at Metro Health District

There is word today of a disturbing data breach at the San Antonio Metropolitan Health District, Newsradio 1200 WOAI reports. Officials say a thief stole a laptop computer which contained the vaccination records of as many as 300 children that are stored in the records of the Vaccines for Children program. *(Are all your devices covered?)*

Alabama Department of Public Health warns of possible data breach

Alabama's Department of Public Health (ADPH) has sent letters to individuals whose personal information may have been compromised and used in a tax fraud scheme. The U.S. Department of Justice's Tax Division informed ADPH of a case which involves the theft of personal information belonging to several entities, including ADPH, the Alabama Department of Corrections, Fort Benning, Ga., and other organizations in the Columbus, Ga., area, according to a victim notification post.

Nearly 70% of critical infrastructure providers suffered a breach

New research from Unisys finds alarming gaps in the security of the world's critical infrastructure. Nearly 70 percent of companies surveyed that are responsible for the world's power, water and other critical functions have reported at least one security breach that led to the loss of confidential information or disruption of operations in the past 12 months. In a survey of 599 security executives at utility, oil and gas, energy and manufacturing companies, 64 percent of respondents anticipated one or more serious attacks in the coming year.

MISO data breach latest in hackers' efforts to reach power grid

Operating cost data from participants in a Carmel-based power network stretching from the Midwest to the Gulf Coast was compromised in a computer breach that highlighted the rising vulnerability of the U.S. electricity infrastructure. Midcontinent Independent System Operator Inc. said it was notified June 26 that a computer server tied to its independent monitor was breached.

HALL ASSOCIATES

P.F. Chang's hit with class-action lawsuit following breach

A proposed class-action lawsuit has been filed against P.F. Chang's China Bistro Inc. by consumers claiming that the restaurant chain failed to protect their personal financial data. The suit, filed Thursday by plaintiff John Lewert on behalf of those affected by the recent data breach, alleges that the company failed to be in compliance with the Payment Card Industry Data Security Standard, and that it knowingly violated its obligation to protect the data "in an effort to save money by cutting corners," according to the complaint filed in the U.S. District Court. *(Is your POS compliant with PCI standards?)*

Greenwich Car Wash Data Breach Could Trouble Thousands

Computer software installed in credit card readers at Splash car washes in Greenwich, Cos Cobb, Stamford, Darien, Norwalk, Fairfield and Wilton could have exposed thousands of customers to identity theft, according to Patch.com. The data breach exposed information from some customers between Feb. 28 and May 16. Officials from Splash say 1,400 customers have been impacted by the breach so far, but the number could swell to more than 30,000 due to the number of patrons potentially exposed to the malware, Patch.com reported. *(Where is your customer's data stored?)*

Computer breach at Houston luxury hotel impacts thousands

At least 10,000 customers of The Houstonian Hotel, Club & Spa were exposed in a credit card security breach that lasted nearly six months, officials alerted guests on Tuesday. The west Houston luxury retreat emailed 10,000 people about the "malicious software attack," which started on December 28, 2013 and continued until June 20, information technology director Jason Love said.

Park Hill data security breach affects more than 10,000 students and employees

The Park Hill School District has notified more than 10,000 current and former district employees and students that a data security breach may have compromised their personal information. The information included Social Security numbers, student records, personnel information and employee evaluations, the district said Tuesday.

Goldman says client data leaked, wants Google to delete email

Goldman Sachs Group Inc said a contractor emailed confidential client data to a stranger's Gmail account by mistake, and the bank has asked a U.S. judge to order Google Inc to delete the email to avert a "needless and massive" breach of privacy. The breach occurred on June 23 and included "highly confidential brokerage account information," Goldman said in a complaint filed last Friday in a New York state court in Manhattan.

Indiana College Warns Staff, Students of Data Breach

Butler University officials are warning more than 160,000 students, faculty, staff and alumni that hackers may have accessed their personal information. The Indianapolis school learned about the data breach when California officials contacted them last month to inform them that they'd arrested an identity theft suspect who had a flash drive with Butler employees' personal information on it. Butler spokesman Michael Kaltenmark said school officials have found that the exposed information includes birthdates, Social Security numbers and bank account information of about 163,000 students, faculty, staff, alumni and even prospective students who never actually enrolled in classes at Butler.