Attorney Advertising

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

Petya Ransomware Attack Has No Kill Switch

On the heels of the WannaCry ransomware attack last month, a new ransomware variant, Petya, hit organizations around the world on Tuesday and stopped them in their tracks—including a major law firm. This keeps us up at night, and we have empathy for our colleagues. It also has affected at least one U.S. nuclear plant's computer system.

Petya encrypts a computer's hard disk to lock out users, and then posts a ransom demand of $300, payable in bitcoin. It is called a "worm" because it has the ability to self-propagate. It infects computers through an exploit called EternalBlue, designed to use a vulnerability in Windows operating systems. A kill switch for WannaCry was discovered by a security researcher, which helped stop the spread of the WannaCry ransomware. However, no kill switch is available for Petya. *Read more*

Health Care Data Breaches Cost $380 per Record

A new study issued by Ponemon Institute, sponsored by IBM, reveals that health care data breaches still cost more than in other sectors.

The Ponemon Institute's calculation is that the average health care data breach costs $380 per record. This compares to the average global cost of $141 per record. This calculates to an average global cost of a data breach or $3.62 million. This is a closely watched benchmark, particularly in determining the cost of cyber liability insurance. *Read more*

ENFORCEMENT + LITIGATION

Anthem Settles Data Breach Suit for Record $115 Million

Anthem Inc. has reportedly agreed to pay a settlement of $115 million to its customers affected by what is being called one of the largest

June 29, 2017

FEATURED AUTHORS:

Kelly Frye Barnett
Linn Foster Freedman
Kathryn M. Rattigan

FEATURED TOPICS:

Children's Privacy
Cybersecurity
Drones
Enforcement + Litigation
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

data breaches in U.S. history.

The settlement is reportedly the largest ever to result from a data breach in the United States and would end a class action lawsuit that commenced after the 2015 breach. Using a stolen password, hackers were able to break into an Anthem database and steal close to 80 million records containing sensitive information belonging to former and current customers, including customer names, dates of birth, physical and email addresses, medical IDs, and Social Security numbers. *Read more*

CHILDREN'S PRIVACY

FTC Issues Update on COPPA

Last week, the Federal Trade Commission (FTC) issued a six-step compliance plan to help businesses comply with the Children's Online Privacy Protection Act (COPPA). It provides clarity on who is covered by, and must comply with, COPPA and how companies can get parental consent. It also outlines a six-step compliance plan. *Read more*

DRONES

Another Drone Bill Seeking Local Control of Drones

We previously wrote about the Drone Federalism Act that was introduced earlier this month. Now another bill is seeking to regulate drones at the local level. The Drone Innovation Act, H.R. 2930, introduced by Congressman Jason Lewis of Minnesota, addresses the operation of drones below 200 feet in altitude "within the lateral boundaries of a state, local or tribal government's jurisdiction." While the proposed bill recognizes that the Federal Aviation Administration (FAA) "retains control over the national airspace," it also directs the U.S. Department of Transportation (DOT) to "work with state and local officials to develop a framework for local operation…to encourage innovation and protect privacy." *Read more*

PRIVACY TIP #94

Keep Your Day Job and Stay Out of Jail

One of my favorite lines when I conduct employee education about data privacy and cybersecurity is "Keep Your Day Job." The context of the comment is when I tell audiences about the dumb moves of employees who think they can steal their company's data and use it,

sell it or do nefarious things with it without getting caught.

Why do employees continue to think that their employers don't monitor their email usage? It is a basic premise that your company will monitor your email traffic when you are terminated or resign. So when I say "keep your day job," I mean, "don't send company data to your private email account or disclose it, steal it, or sell it."

It continues to amaze me how often this happens. And it puts both the company and the employee in a precarious position.

Take the former litigation associate of a major law firm who was arrested late last week on an extortion charge. Although the associate was smart enough to go to law school, he wasn't very smart in his scheme.

This associate threatened the law firm that he would release confidential and sensitive data from his superior's email account unless the firm paid him $210,000 and gave him a piece of art.

What? Really? How did he think he would not get caught?

The tip for this week: keep your day job. Don't steal or disclose your company's data. Don't sell it or extort your company. Chances are you will get caught and no longer have a job or be employable.