Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

Federal Agencies Hit with 30,899 Cyber Incidents in 2016

The Office of Management and Budget (OMB) released a report this week indicating federal agencies experienced almost 31,000 cyber incidents in 2016. Despite the dismal number of incidents, the report noted the situation is improving because agencies are implementing more sophisticated data security measures, including two-factor authentication, and identifying and protecting high-risk data. *Read more*

DATA PRIVACY

House Bill Would Allow Employers to Require and Access Genetic Testing Results

House Bill HR 1313, introduced by Representative Virginia Foxx (R-N.C.), proposes to allow companies to require employees to undergo genetic testing, then allow employers to see the results, and impose financial penalties on any employees who request to opt out of the requirement. Those in support of the bill state that the legislation would give employers the ability to offer wellness plans, promote a healthy workforce, and lower health care costs. *Read more*

DATA BREACH

Air Force Security Clearance Files Compromised on Unsecured Backup Drive

Security researchers have discovered that an unsecured backup drive has compromised thousands of U.S. Air Force documents, including personnel files and sensitive forms filled out by senior and high-ranking officials. These files were openly accessible because they were located on a backup drive which was connected to the Internet but wasn't password protected. *Read more*

March 16, 2017

FEATURED AUTHORS:

Linn Foster Freedman
Kathryn M. Rattigan

FEATURED TOPICS:

Cybersecurity
Enforcement + Litigation
Data Breach
Data Privacy
Drones
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

Cardiology Group Hard Drive Stolen

Denton Heart Group, located throughout Dallas, has notified 21,665 patients that their protected health information has been compromised as a result of the theft of a hard drive from a locked closet.

The hard drive in the closet contained the group's backup data from the practice's electronic health system—which included apparently of all of its patients' information over the span of eight years. *Read more*

Home Depot Settles with Financial Institutions

A federal judge has preliminarily approved a proposed settlement of $25 million between Home Depot and financial institutions that issued payment cards affected by the Home Depot data breach in 2014. This proposed settlement amount is in addition to the $140 million settlement with other payment card issuers, such as American Express and Discover, through card brand recovery processes. *Read more*

DRONES

UAS, a Growing Part of the Oil and Gas Industry

As the use of unmanned aerial systems (UAS or, as they are more commonly called, drones) continues to rapidly increase as technology continues to develop, more industries will utilize UAS in their day-to-day operations, including the oil and gas industry. Initially, UAS were mainly used in the oil and gas industry for conducting inspections, but now, UAS are becoming part of the fabric of the industry. UAS are used for a variety of tasks, from monitoring pipelines to providing assistance during oil spills. *Read more*

ENFORCEMENT + LITIGATION

Wendy's Executives and Board File Motion to Dismiss

We previously reported that Wendy's was hit with a putative class action shareholders' derivative suit in December following its data breach in 2016 [view related post]. Late last week, the executives and board of Wendy's filed a motion to dismiss the case, saying the allegations in the complaint were pure speculation and the plaintiff failed to allege that the board acted with gross negligence or reckless disregard of its duties or that it failed to monitor Wendy's data security

measures, or disregarded security vulnerabilities. *Read more*

PRIVACY TIP #78

Cybersecurity Aids for Small Businesses

I frequently get complaints from small businesses that they don't have the resources or resilience to properly address cybersecurity and it is overwhelming to them.

Well, it is. We frequently tell businesses they must be prepared, as they might not think they are targets, but they are. But what happened to the relevance of the concept of "according to the size and scope of the entity?"

On March 10, 2016, the House Small Business Committee issued new cybersecurity aids for small businesses following a hearing that emphasized their vulnerabilities.

The statistics are quite alarming: almost 60 percent of small companies go out of business in the wake of a hacking incident, and 71 percent of all cyber assaults happen in businesses with less than 100 employees.

The guide is split into three parts. The first relates to data breach response and basically refers businesses to the FTC guidance on the topic.

The second is targeted to small vendors and Internet of Things products and outlines measures to protect themselves and their customers.

Another section outlines five things small companies can do to protect personal information. They include:

- Take stock—map and know where personal information is and when it is on Web-connected computers.
- Scale down—keep only the information the business needs
- Lock it—know how to protect the information.
- Pitch it—know how to properly dispose of personal information when it is no longer needed.
- Plan ahead—know how to develop a security incident response plan.

These are basic, but sound, measures that small businesses can take to protect themselves and get the overwhelming process started so it doesn't seem so difficult. It's worth a read.