Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

NIST Issues Practice Guide for Electric Utilities

On February 16, 2017, the National Cybersecurity Center of Excellence released its draft practice guide for electric utilities, titled Situational Awareness for Electric Utilities.

The guide was developed to provide an example solution that can be used by electric utilities to alert staff to the potential for or an actual cyber-attack directed at the electric grid. *Read more*

Sony Cyber-Attackers Lurking at Financial Supervisor "Watering Hole" Target Banks and Others

Cybersecurity specialists at BAE Systems and Symantec new evidence announced last week suggesting that the criminals behind the notorious 2014 attack on Sony Corp. are also responsible for recent cyber-attacks involving 104 organizations in 31 countries. Researchers and investigators have long attributed the 2014 Sony attack, which crippled computer systems and revealed internal emails, to the North Korea-linked group known as "Lazarus." Malware recently discovered running on the computers of a Polish bank s uggest that the Lazarus group is now targeting global financial institutions using a sophisticated "watering hole" technique. *Read more*

New York Financial Services Cybersecurity Regulations Go into Effect on March 1

We have previously reported about the upcoming New York Financial Services Cybersecurity Regulations [view related posts here and here]. On February 16, 2017, Governor Andrew M. Cuomo announced that "the first-in the-nation cybersecurity regulation to protect New York's financial services industry and consumers from the ever-growing threat of cyber-attacks will take effect on March 1, 2017." *Read more*

February 23, 2017

FEATURED AUTHORS:

Scott M. Baird
Nuala E. Droney
Linn Foster Freedman
Kathryn M. Rattigan
Norman H. Roos

FEATURED TOPICS:

Cybersecurity
Enforcement + Litigation
Data Breach
Data Privacy
Drones
HIPAA
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

HIPAA

Report Lists Health Care Data Breaches by State

A new report issued by Safetica USA has organized data breaches affecting over 500 individuals that were self-reported to the Office for Civil Rights (OCR) in 2016 into a list by state and records exposed. *Read more*

$5.5 million Shelled Out to OCR for Alleged HIPAA Violations

Florida Memorial Healthcare Systems has agreed to pay the Office for Civil Rights (OCR) $5.5 million to settle alleged HIPAA violations relating to an incident that occurred in April, 2012, where two employees accessed patient information of 106,000 patients in an unauthorized manner and with criminal intent, including their names, dates of birth, and Social Security numbers. This penalty matches the largest penalty paid to OCR so far, which was paid by Advocate Health Care. *Read more*

Report Summarizes Health Care Data Breaches in January 2017

Health care data breaches are not slowing down. According to a report issued by Protenus, in conjunction with www.databreaches.net, the summary of health care data breaches in 2017 continues where 2016 left off. In January 2017, there were 31 data breaches reported to the Office for Civil Rights. The breaches resulted in the compromise of 388,307 patient and health plan members' Personal Health Information (PHI). *Read more*

ENFORCEMENT + LITIGATION

FTC and Ten States Settle with Caribbean Cruise Lines for Robocall Accusations

This week, the Federal Trade Commission (FTC) and ten states settled charges against the Florida-based cruise line, Caribbean Cruise Line, (CCL) Inc., for an illegal telemarking campaign that inundated consumers with billions of unwanted robocalls. *Read more*

DATA BREACH

Yahoo Data Breach Update: A Third Notification and

Shareholders Sue

Last week, Yahoo issued another warning to some of its customers telling them that their personal information may have been compromised in a data breach. This is the third notification to Yahoo users that their information has been exposed [view related posts here and here]. The breach is reported to be the largest in history. *Read more*

W2 Phishing Scam Hits Citizens Memorial Hospital

We continue to see all industries hit with W2 phishing scams, including the health care industry.

Citizens Memorial Hospital, located in Bolivar, Missouri, was hit with the scam when one of its employees believed that an email received from another employee was legitimate and sent the W2s of its employees from 2016 to a hacker. *Read more*

DATA PRIVACY

The Defend Trade Secrets Act of 2016: A Year Later by the Numbers

It has been almost a year since the Defend Trade Secrets Act of 2016 (DTSA) took effect. Because *Forbes Magazine* called the DTSA the "Biggest IP Development in Years," we thought it might be helpful to take a look at how often litigants have chosen to use it in federal cases this past year. *Read more*

DRONES

DJI Drone Manufacturer Hit with Class Action Lawsuit over Firmware Update

Last week, a class action lawsuit was filed against a leader in the drone industry, DJI Technology, Inc. (DJI), for an allegedly harmful firmware update that occurred in December 2015 that rendered certain commercial drones in its Phantom 2 line of drones unable to record video or take photographs. DJI is accused of ignoring the injury that thousands of Phantom 2 drone owners faced in light of this damaging update. DJI allegedly refused to reimburse them, replace the product, or take responsibility for the alleged flaw. *Read more*

PRIVACY TIP #75

Yes—Those Tech Support Scams Are Really Scams

My friends and family frequently ask me about the newest scam, so they can stay vigilant and keep on top of the latest ways fraudsters are trying to get our information.

But many times, they alert me to scams that they are experiencing. Such was true this week.

We all know by now it is a scam when people call us on our residential phone line saying they are from "Windows Support." Unfortunately, the Federal Trade Commission (FTC) continues to warn consumers not to give anyone their user names and passwords to get into their computer over the telephone.

But now scammers are getting more creative and have figured out a way to insert a pop-up into your computer. This happened this week to someone I know. He was using his computer when a pop-up message appeared that said his computer was having issues and needed tech support. He says the message looked totally legitimate (and he is well-trained!), so his antennae went up. The pop-up included an 800 number to call. Curious, he called the number and started cross-examining the guy on the other end of the line. When t he guy asked for the user name and password, he knew it was a scam, even though it sounded pretty legitimate. He took his computer to his IT department to check out how the pop-up was inserted. As always, this makes me concerned about vulnerable people such as seniors.

Days later, on February 21, 2017, the FTC blog posted a piece on "Global Connect technical support scam, part 2." The blog reminded us that the FTC shut down an operation called Global Connect, which was behind these pop-ups. It is warning consumers that Global Connect is back at it despite that the FTC "shut it down."

The FTC is asking consumers to let it know if they get one of these pop-ups or calls so it can continue to go after them. For more information about how to detect a tech support scam, visit the FTC website at www.ftc.gov.