Attorney Advertising

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

AICPA Releases Cybersecurity Risk Management Reporting Fact Sheet for CPAs without a Key Recommendation

The American Institute of CPAs (AICPA), has released a risk management reporting framework intended to "establish a common, underlying language for Cybersecurity risk management reporting—almost akin to US GAAP or IFRS for financial reporting. "According to AICPA, the framework may be used by both management and CPAs to "enhance cybersecurity risk management reporting of an organization's cybersecurity efforts." *Read more*

OneLogin Suffers and Notifies Customers of Very Sophisticated and Scary Intrusion

San Francisco-based OneLogin, which provides single sign-on and identity management services for companies and app vendors, recently notified its users that it has discovered an unauthorized access to its data. The idea behind OneLogin is for a user to have one username and password that it can use through OneLogin's platform for all of the user's apps. This makes sign-on easy for users but means all of the user's apps can be compromised if the single sign-on authentication is compromised. This risk is exactly what happened in this incident. *Read more*

HEALTH INFORMATION

"Fireball" Malware a Threat to Health Care Industry

A new report released by Check Point has security personnel working in the health care industry particularly concerned, and they are warning their colleagues about the existence of Fireball. Released by a Chinese operation, Fireball has infected approximately 250 million computers worldwide. According to the report, the malware hijacks web browsers and turns computers into "zombies" and then manipulates the user's browsers and changes default home pages and search engines into fake ones. It can also execute code on the user's machine, which allows the hackers to steal the user's credentials. It also has the capability to spy on users and to exfiltrate sensitive information. *Read more*

June 8, 2017

FEATURED AUTHORS:

Kelly Frye Barnett
Linn Foster Freedman
Joanne J. Rapuano
Kathryn M. Rattigan

FEATURED TOPICS:

Cybersecurity
Data Breach
Data Privacy
Drones
Enforcement + Litigation
Health Information
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

HHS Releases Health Care Industry Cybersecurity Task Force Report

This week, the Department of Health and Human Services (HHS) issued its *Report on Improving Cybersecurity in the Health Care Industry*, a culmination of a year-long effort on behalf of the Cybersecurity Task Force, which is made up of industry professionals from the public and private sectors to identify and develop recommendations "on the growing challenge of cyber-attacks targeting health care." *Read more*

OCR Issues Reminder on Security Incidents

Following the frequent and varied ransomware attacks on health care entities over the past few years, the Office for Civil Rights (OCR) published guidance last summer for the health care industry, reminding it that a ransomware attack could be a reportable breach under the HIPAA Breach Notification Rule. Despite the fact that many health care organizations were victims of ransomware attacks, the OCR commented that many of them did not report the incident or notify patients of the incident. *Read more*

ENFORCEMENT + LITIGATION

U.S. Supreme Court Will Hear Mobile Phone Privacy Case

The United States Supreme Court has just agreed to hear the case of a Detroit man sentenced to 116 years in prison after data from his own cellular phone was used against him at his trial for his role in a string of robberies of Radio Shacks and T-Mobile stores in metro Detroit and Ohio over a two-year period. Timothy Ivory Carpenter, who was sentenced in 2014 in U.S. District Court, was alleged to have organized the robberies, and cell phone data obtained without a warrant from his provider was presented at his trial. The data indicated, according to an expert witness, that he was in the vicinity of the robberies when they occurred. *Read more*

A&B Insurance Settles TCPA Class Action for $4.25 Million

Last week, A&B Insurance and Financial LLC (A&B Insurance) agreed to pay $4.25 million to settle claims it violated the Telephone Consumer Protection Act (TCPA) by initiating telephone calls to consumers without prior express consent, as required by the TCPA, including some calls to consumers on the federal Do Not Call Registry. Lead plaintiffs, Jim Youngman and Robert Allen, claimed that A&B Insurance (through a third-party vendor) made prerecorded calls to their cell phones. *Read more*

DATA PRIVACY

To Travel with My Laptop…or Not!

Tricky decision to make if you are among the millions that travel for work…. how safe is it? Will the new laptop travel ban affect me? What airports am I connecting through that are of concern? Is public Wi-Fi secure? Did that person just look over my shoulder (a.k.a. shoulder surfing) while I was opening an email with client information all over it? Some examples of reported incidents include full disk copies made while the laptop owner was out of the hotel room, laptops stolen at security screening lines, wireless access services monitored by third parties to gain information transmitted through Wi-Fi service, malicious software installations (including viruses), and programs that capture log-in data and automatically transmit key data to other locations. *Read more*

DATA BREACH

2,500 Mothers' and Newborns' Personal and Health Information Lost in the Mail

The Arizona Department of Health Services (ADHS) has notified 2,500 patients that their personal and health information has been lost in the mail. The affected patients were mothers and newborns enrolled in the newborn screening program operated by ADHS. The compromised information was contained on paper records, including names, addresses, Social Security numbers, health insurance information, dates of birth, and telephone numbers, which was placed in two boxes and sent via U.S. mail from Phoenix, Arizona, to Carbondale, Illinois, for billing purposes. One box arrived at the destination, and the other didn't. The last time the box was tracked, it was located at the Phoenix U.S. Postal Service facility. However, it hasn't been located. *Read more*

DRONES

Drone Federalism Act, Seeking Regulation of Drones at the Local Level

The Drone Federalism Act of 2017, introduced by U.S. Senators Dianne Feinstein, Mike Lee, Richard Blumenthal, and Tom Cotton, seeks to "establish a process for federal, state, local and tribal governments to work together to manage the use of recreational and commercial drones." This bill would allow "communities to create low-altitude speed limits, local no-drone zones or rules that are appropriate to their own circumstances." *Read more*

PRIVACY TIP #91

Teen App Wishbone Compromised—Female Teenagers at Risk

Social networking app Wishbone, used primarily by teenage-girls to vote on various teenage type quizzes, like favorite entertainers or fashion, has been hacked.

The intruders have reportedly gained access to users' (again, primarily female minors) names, unique email addresses, and mobile telephone numbers. Not just a few, either. The data compromised included 2,326,452 full names, 2,247,314 unique email addresses, and 287,502 mobile telephone numbers. Some dates of birth and gender information were also compromised.

Email addresses are concerning as that is the method hackers use to create phishing emails that introduce malware and ransomware into users' systems or attempt to engage the users in email conversations for nefarious purposes. Even more concerning is the fact that the hackers got ahold of hundreds of thousands of teenage girls' cell phone numbers. As a parent, this should be very concerning.

If you have a teenager, and in particular a teenage girl who uses Wishbone, the teenager should be alerted to this compromise and educated on the risks of phishing schemes, malware and ransomware, engaging in online conversations with people they don't know, and engaging in telephone conversations with strangers. All of this online behavior is risky, but the fact that unique email addresses and cell phones numbers have been compromised puts these individuals at an even higher risk that they will be targeted.