Attorney Advertising

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

Verizon's Protected Health Information Data Breach Report Concludes that Insiders Are Greatest Threat to Health Care Entities

Verizon recently issued its Protected Health Information Data Breach Report, which is always an interesting read. Not surprisingly, Verizon's report concludes that, based upon analysis of 1,360 security incidents involving the health care sector, 58 percent of the incidents were caused by insiders and 42 percent were caused by external threats. *Read more*

473,807 Patient Records Compromised in January, 2018—83 Percent Caused by Hacking Incidents

The recently released Protenus Healthcare Breach Barometer Report notes that in January 2018, at least 473,807 patient records were compromised in 37 breaches reported to the Office for Civil Rights. Twelve of the reported breaches were attributable to insiders, which was 32 percent of the data breaches reported in January. Seven of those incidents were caused by insider error and five were caused by wrongdoing. This type of incident shows how important employee education and monitoring continues to be in detecting and mitigating breaches caused by employees. *Read more*

DATA BREACH

Last Two States Considering Passage of Data Breach Notification Laws

The last two states which have not passed data breach notification laws are Alabama and South Dakota. Sometimes we make jokes about these states, as they are so late to the data breach notification table (California was the first state to pass a data breach notification law in 2002) and they seem not to care about consumer protection.

Not so anymore. Both Alabama and South Dakota are considering passing data breach notification laws. *Read more*

ENFORCEMENT + LITIGATION

March 15, 2018

FEATURED AUTHORS:

Linn Foster Freedman
Jessica A.R. Hamilton
Kathryn M. Rattigan

FEATURED TOPICS:

Cybersecurity
Data Breach
Drones
Enforcement + Litigation
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

Flying with Your Data—ACLU Sues the TSA Over Domestic Electronic Device Searches

If you've flown domestically in the last year, you know the drill. Take off your jacket, belt, and shoes and place them in a bin. Remove your quart-sized bag of 3.4 oz liquids and place them on top. Pull out your laptop, iPad, e-reader, gaming device, and any other electronic device larger than a cell phone, and place them in another bin. Shuffle through the full body scanner while keeping an eye on your belongings, then pack everything back up before heading to your flight. But what about all the data on your electronic devices—is that subject to a search? *Read more*

Facebook Can't Shake Illinois Biometric Proposed Class Action Case

We have previously reported on Facebook's fight against a proposed class action case alleging violation of the Illinois Biometric Information Privacy Act (BIPA). Facebook continues to fight the allegation that its collection and storage of users' and non-users' facial scans through the use of facial recognition technology violates BIPA, and has filed a Motion to Dismiss the case which is pending in California (after it was successful in having the case transferred to California from Illinois). *Read more*

DRONES

Massive Adoption of Drones; Safety Still Top Concern for Officials

At the Association for Unmanned Vehicle Systems International (AUVSI) and Federal Aviation Administration (FAA) co-hosted Unmanned Aerial Systems (UAS or drones) Symposium in Baltimore, Maryland last week, all speakers agreed on one thing: safety is the primary concern. *Read more*

FAA Plans to Bring LAANC to 500 More Airports by Next Month

On March 6, 2018, the Federal Aviation Administration (FAA) announced the nationwide expansion of its Low Altitude Authorization and Notification Capability (LAANC) to 500 more airports, and include 300 air traffic control facilities as well as open up 78,000 miles of previously restricted airspace to commercial drone flights. Under FAA Part 107 drone regulations, operators must secure approval from the FAA to operate in any airspace controlled by an air traffic facility. *Read more*

JHUISI Creates New Way to Protect Drones from Cyber-Attacks

OnBoard Security, a Wilmington, Massachusetts-based security provider, announced last week that graduate students from Johns Hopkins University Information Security Institute (JHUISI) have successfully implemented a secured type of sense-and-avoid (SAA) technology for drones to prevent mid-air collisions, which is not as

vulnerable to cyber-attacks as other prior SAA technologies. *Read more*

PRIVACY TIP #130

Smartphones Targeted by Dark Caracal Attack

There is a global malware campaign that is targeting mobile devices across the world. It is called Dark Caracal, which is believed to be sourced in Beirut by the Lebanese General Security Directorate. According to security researchers, attacks on mobile devices are on the rise because people are using their smartphones more than they are using laptops or desktop computers, and there is more information on smart phones than on other devices.

The malware is disguised as a messaging app like Signal and WhatsApp. It asks the user to authorize permission to take photos, access the microphone and location based services, so the user is tricked into believing that it is a real app, and as the user always does, clicks "yes" to every pop-up that a new app presents, which then gives the intruders full access to the phone. According to the researchers, this app is not "exploiting a code's vulnerabilities, it's exploiting a person's vulnerabilities." We can be our own worst enemy.

The good news is that the Google and Apple app stores are working hard to keep these apps out of its stores, but the same is not true for third-party app stores. Dark Caracal spread by advertising on websites and group sites. The tip is not to download an app through a third-party app store.

Another tip is to apply any security patches issued by a manufacturer as soon as possible. According to a report issued by the FTC in February, individuals are not patching vulnerabilities to their smartphones quickly enough and are becoming victims of already disclosed vulnerabilities because they are not updating their phones with security patches issued by manufacturers.

So next time your phone asks you to update to the next operating system, don't say "later." Do it now.