Robinson+Cole

Data Privacy + Cybersecurity Insider
Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

iPhone Users Targeted by New Malware Campaign

Cisco Talos has discovered a new menace to iPhone users—a sophisticated malware campaign targeting iPhones to trick users into downloading an open-source Mobile Device Management (MDM) solution that gives the hackers control of the phone. It is reported that Cisco and Apple are working together to combat the threat. According to reports, once the MDM tool is downloaded and the hackers have control of the phone, they can steal information from the infected devices, including the phone number, serial number, location, contact information, and basically everything else on the phone. *Read more*

Malware Attacks Up 75 Percent According to New Report

A new report issued by Positive Technologies finds that cyber incidents have increased 32 percent from the first quarter of 2017 to the first quarter of 2018. It also notes that the theft of account credentials is on the rise. Alarmingly, the report states that the greatest increase in cyber-attacks was the use of malware attacks, which increased 75 percent from the first quarter of 2017 to the first quarter of 2018, and that malware was used in 63 percent of all attacks. *Read more*

DATA PRIVACY

MLB to Use Biometrics to Replace Traditional Ticketing

Traditional tickets (paper that is) have already been replaced with mobile tickets for many Major League Baseball (MLB) stadiums across the country, but now, MLB has teamed up with CLEAR, which provides biometric authentication, to implement biometric ticketing at select stadiums. CLEAR will allow baseball fans to use their fingerprints, and eventually facial recognition, to enter the stadium. This program will begin later this season, and the full rollout will happen sometime next season. *Read more*

July 19, 2018

FEATURED AUTHORS:

William M. Daley
Linn Foster Freedman
Kathryn M. Rattigan
Matthew W. Rizzini

FEATURED TOPICS:

Cybersecurity
Data Privacy
Drones
Health Information Privacy
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

HEALTH INFORMATION PRIVACY

[Health Care Industry Continues to Fight Cyber-Attacks at Alarming Rate—Health Care Data Breaches Cost Average of $408 Per Record](#)

It is clear that the health care industry continues to be targeted with cyber-attacks. In 2018, the 10 largest health care breaches, [outlined here](#), include unauthorized access to Protected Health Information (PHI) through a vendor offering claims processing, ransomware incidents, successful phishing schemes, mailing PHI to wrong addressees, hacking, a misdirected email, and a lost unencrypted hard drive. Most of these might have been prevented through greater employee security awareness. *Read more*

[Massachusetts PATCH Act, Requires Additional Protection for Certain Confidential Health Care Information](#)

Earlier this year, Governor Charlie Baker signed into law an Act to [Protect Access to Confidential Healthcare](#) (the "PATCH Act"), which prevents information regarding "sensitive health care services" from being shared with anyone other than the patient in the form of Explanation of Benefits (EOB) and Summary of Payment (SOP) forms. When more than one person is covered by the same medical insurance plan, sensitive health care information can be disclosed through the use of these common forms, sometimes including information on sexual assault, domestic violence, mental health disorders, or sexual and reproductive health. When the EOB or SOP is provided to the named policyholder—rather than the specific beneficiary that the services described therein relate to—the beneficiary's confidentiality can be compromised. *Read more*

DRONES

[DJI Enhances Geofencing Flexibility in its Drones](#)

DJI, a leading drone manufacturer, has announced its strengthened commitment to enterprise drone users with new improvements to its geofencing system. Professional drone pilots with authorization to fly in sensitive locations can now use a streamlined application process to receive unlocking codes within 30 minutes. DJI's geofencing systems uses GPS and other navigational satellite signals to automatically help prevent drones from flying near sensitive locations like airports, nuclear power plants and prisons. These improvements are carefully designed to help expand the uses of drones in sensitive areas that have been restricted in DJI's geofencing system. While those sensitive areas will remain restricted for drone hobbyists (i.e.,

non-commercial pilots), DJI will now staff its global authorization team 24-hours a day. *Read more*

PRIVACY TIP #148

Medtronic MyCareLink Heart Monitors Vulnerabilities Identified

Wearable technology and medical devices have vulnerabilities just like anything else that is digital. This week's privacy tip focuses on a recent advisory about vulnerabilities in Medtronic's MyCareLink patient heart monitors. *Read more*

Boston | Hartford | New York | Providence | Stamford | Albany | Los Angeles | Miami | New London | rc.com

Robinson & Cole LLP