Attorney Advertising

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

Hackers Could Target Airports, Planes, Satellites, Ships, Cars, and Trains

Cybersecurity for critical infrastructure continues to be of concern, including the transportation sector. A new study by ABI Research concludes that, although the transportation sector continues to increase spending on cybersecurity year after year, the rapid digitization of airports, aircraft, trains, ships, and cars puts this sector at risk.

The study mentions that poor cybersecurity is being applied to operational and control systems in the transportation sector, including engine and flight control systems, electronic positioning systems, logistical systems, communications systems, and navigational systems, and because many of them use off-the-shelf software and connect to the Internet via Wi-Fi or cellular networks, they are susceptible to hacking and intrusion. *Read more*

Students 16 and Over: Check Out CyberStart!

Students 16 years old and over who live in Virginia, Michigan, Iowa, Hawaii, Nevada, Delaware, and Rhode Island—you may be eligible to participate in a new cybersecurity skills program called CyberStart. You need access to the Internet and a computer to participate.

CyberStart is "a forward-thinking skills program designed to supply specialist cyber security education to young people across the U.S. Using a suite of online challenges, tools, and games, it aims to inspire the next generation of cyber security professionals whilst identifying the best and most talented young Americans."

Registration is open until August 4, and you have to qualify first before you can participate in the full program, so act quickly. The registration link is here.

DATA BREACH

Data Breach at Italy's No. 1 Bank Exposes 400,000 Accounts

Italy's top bank, UniCredit SpA, is yet another victim in a series of cyber-attacks exploiting vulnerabilities in the financial services industry. Criminals made off with biographical and loan data from 400,000 UniCredit loan accounts after gaining access to the bank's computer system through one of it's third-party commercial partners. The series of data breaches was discovered after an internal IT check

August 3, 2017

FEATURED AUTHORS:

Linn Foster Freedman
Kathryn M. Rattigan
Norman H. Roos
Scott N. Siedor

FEATURED TOPICS:

Children's Privacy
Cybersecurity
Data Breach
Drones
HIPAA
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

showed that some of the third-party partner's users were accessing sensitive UniCredit data. *Read more*

Women's Health Care Group Notifies 300,000 about Ransomware Attack

Women's Health Care Group of Pennsylvania has notified approximately 300,000 patients that their protected health information has been compromised by a ransomware attack.

Although the ransomware became active on May 16, 2017, an investigation into the attack showed that the intruders had access to the group's system since January of 2017. The intruders may have had access to patients' names, Social Security numbers, birthdates, pregnancy history, lab results, insurance information, and diagnoses. Once the ransomware was discovered, the information was restored through use of the group's back-up system.

HIPAA

OCR Releases "Improved Web Tool" for Breach Reporting

The Office for Civil Rights (OCR) recently issued an "improved web tool that puts important information into the hands of individuals, empowering them to better identify recent breaches of health information and learn how all breaches of health information are investigated and successfully resolved." The tool, "the HIPAA Breach Reporting Tool (HBRT), allows individuals to navigate the breach reporting website so they can find information relating to data breaches and allows organizations to report a data breach with more ease. *Read more*

DRONES

FAA Reauthorization Bill: What does it mean for the UAS legal landscape?

In the last few weeks, the Federal Aviation Administration (FAA) Reauthorization bills have made their way around both houses of Congress, which will allow funding to the FAA to continue beyond Fall 2017. These bills contain lengthy and significant language that could greatly affect commercial and hobbyist drone operations in the U.S. Below is a summary of the main provisions in the House's bill:

- UAS Traffic Management (UTM) System: Directs the FAA to initiate rulemaking within 18 months to establish procedures for issuing air navigation facility certificates to operators of low-altitude UTM systems.

- Risk-Based Permitting Process: Establishes a risk-based permitting process to authorize UAS operations that meet certain safety standards. *Read more*

North Carolina Introduces New Drone Bills

North Carolina Governor Roy Cooper signed two bills this week to regulate the use of unmanned aerial systems (UAS or drones). First, House Bill 337 revises existing state drone law to make it applicable to model aircraft. House Bill 128 prohibits drone use near prisons – with the term "near" being defined as a horizontal distance of 500 feet or a vertical distance of 250 feet. Both of these bills will go into effect on December 1, 2017. *Read more*

Contraband Drone Crashes Near Prison in Washington State

Last week, a drone carrying 16 individual bags of marijuana, cell phones and chargers, two bags of tobacco, and 31 oxycodone pills crashed into the ground near the Washington State Prison yard.

A corrections department spokeswoman, Joan Heath, said that the drone crashed into the ground near the prison around 10:45 p.m. Drones carrying contraband into prison yards has been a growing problem. *Read more*

Part 107 Waivers: Does Your Waiver Stand a Chance?

The Federal Aviation Administration's (FAA) Part 107 waiver process for the operation of unmanned aerial systems (UAS or drones,) in certain restricted airspace or beyond the limitations of the Part 107 UAS regulations, was originally designed to streamline approval. However, for many drone operators who have had their Part 107 waivers denied, the process can often be mysterious and frustrating. And the FAA's public database of all approved Part 107 waivers, while useful, does not include denied waivers, which could be key for many operators in determining what information is necessary and what safety processes the FAA desires for obtaining an approval. *Read more*

CHILDREN'S PRIVACY

FTC Approves Modifications to TRUSTe's COPPA Safe Harbor Program

The Federal Trade Commission (FTC) approved TRUSTe's proposed modifications to their Children's Online Privacy Protection Act (COPPA) safe harbor program this week.

COPPA requires, among other things, that commercial website and mobile app operators who knowingly collect personal information from children under age 13 post comprehensive privacy policies on their websites and in their mobile apps, notify parents and guardians of the website's or mobile app's information practices, and obtain parental consent before collecting, using, or disclosing any personal information from children under age 13. However, COPPA includes a safe harbor provision whereby industry groups may seek approval from the FTC to create self-regulatory guidelines that implement "the same or great protections for children" as those in COPPA. Website and mobile app operators who participate in FTC-approved safe harbor programs are subject to the review and disciplinary procedures

provided in the safe harbor guidelines in lieu of an FTC's formal investigation or enforcement. *Read more*

PRIVACY TIP #99

If You Are an IoT Fanatic, This App Is for You

Last January, the Federal Trade Commission (FTC) launched the IoT Home Inspector Challenge, a contest that requested participants to come up with a tool that would identify security issues caused by out-of-date software in IoT devices to better educate and protect consumers about the security vulnerabilities of IoT devices.

To remind you of all of the "things" that may be connected to the Internet, we have previously flagged the security risks of IoT things, including dolls, toys, security systems, refrigerators, cars, stoves, coffee makers, washing machines, and even aquariums. Anything connected to the Internet can be hacked, accessed, and manipulated.

The FTC recently announced the winner of the IoT Home Inspector Challenge—Steve Castle—who developed a mobile app called IoT Watchdog. IoT Watchdog scans an individual's Wi-Fi and Bluetooth networks to assemble a list of IoT devices for the individual, identifies those devices that have out-of-date software or other vulnerabilities, and provides instructions to the user about how to update the software or fix the vulnerability.

Now that's a great idea. Congratulations to Steve Castle for helping us all better protect our IoT devices and thereby protect our privacy from malicious actors.