Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

St. Jude Medical on Hot Seat for Cybersecurity Flaws in Home Monitoring System

St. Jude was accused last year by an investment research firm of having lax cybersecurity measures for its Merlin@home monitoring system. The Food and Drug Administration (FDA) recently issued a warning letter to St. Jude Medical, alleging that it failed to properly investigate issues with the batteries in its defibrillator implants and for failing to fix the cybersecurity of its in-home monitoring system, known as Merlin@home. The monitoring system is wireless and is connected to St. Jude's implantable cardiac devices, including pacemakers, defibrillators, and resynchronization devices. *Read more*

ACC Issues Data Security Guidelines for In-House Counsel to Evaluate Law Firms

The Association of Corporate Counsel (ACC) has issued its first-ever data security guidelines, which outline basic data security measures that in-house counsel can use to evaluate their outside counsel. Most companies these days are auditing their law firms' data security measures, but since data breaches occurred at some of the largest U.S. based law firms last year, more attention is being paid to questioning law firms about data security. *Read more*

HIPAA

OCR Levies Hefty Fine against Federally Qualified Health Center

Showing no signs of letting up on enforcement actions, late last week the Office for Civil Rights (OCR) settled an investigation against Metro Community Provider Network (MCPN), a Colorado based federally qualified health center, for alleged HIPAA violations. The fine, was at a whopping $400,000 for the center, which provides health care services to low income patients. It settled alleged HIPAA violations of failing to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI...and to implement security measures sufficient to

April 20, 2017

FEATURED AUTHORS:

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

FEATURED TOPICS:

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

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

reduce risks and vulnerabilities to a reasonable and appropriate level." *Read more*

March Sees an Uptick in Health Data Breaches

The monthly breach report issued by Protenus last week outlining data breaches that occurred in the month of March concludes there was an “uptick in the number of health data breach incidents.” According to the report, there were 39 incidents last month that involved health information, compromising 1.5 million patient records. A whopping 44 percent of the incidents were the result of “insider threat,” which includes both criminal (malicious) and accidental (honest) activity. This number includes the largest incident in March involving the theft of 697,800 records from Med Center Health. *Read more*

ENFORCEMENT+LITIGATION

FTC Resolves Allegations against Three U.S. Based Companies Involving Misrepresentations of International Privacy Program Certifications

Privacy laws in Asia-Pacific countries such as Japan, Australia, New Zealand, and Singapore restrict the export of personal information except when the exporter meets certain qualifying conditions. One qualifying condition is if the exporter is in compliance with the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules System (CBPR). Recently, the Federal Trade Commission (FTC) charged three U.S. companies with violating Section 5(a) of the FTC Act on the grounds they falsely represented in their privacy policy that they were compliant with the APEC’s CBPR. *Read more*

DATA SECURITY

Cops, Cameras, and The Cloud: Axon’s Offer of Free Body Cameras to U.S. Police Departments

Earlier this month, Axon, the company formerly known as Taser, offered a one year free trial of its body cameras and cloud storage to every police department in the United States. While controversy about the use of body cameras is making the news now, controversy about cloud storage for the data captured by those cameras will impact police and prosecutions for years to come. *Read more*

DATA BREACH

InterContinental Hotels Group Reports Credit Card Breach

InterContinental Hotels Group (IHG) has reported a data breach of its payment card processing system. The breach involves malware that infected certain locations between September 29, 2016, and December 29, 2016. The malware lifted customers' names, credit card numbers, expiration date, and the security codes of credit cards used at certain locations during that time frame. Click here for a list of affected hotels organized by state. *Read more*

SWIFT Shores Up Network Security with Real Time Cybersecurity Tools

In an effort to combat an increasing number of fraudulent transfers carried out using its network, SWIFT, the international bank transfer network, announced this month it is adding new tools and controls designed to prevent fraudulent transfers in real time. The new tools integrate into the SWIFT system directly, without the need for new hardware or software, and allow financial institutions to screen SWIFT message flows according to a set of pre-defined parameters. Suspicious money transfer requests are immediately flagged and can be reviewed by a financial institution before processing. *Read more*

DRONES

OIG to Audit FAA Drone Waiver Processes

The Office of the Inspector General (OIG) of the U.S. Department of Transportation (DOT) has announced an audit of the Federal Aviation Administration's (FAA) "approval and oversight processes" for Part 107 waivers for unmanned aerial systems (UAS) operations. The audit will begin before month's end and will assess the FAA's processes for granting waivers and its "risk-based oversight" for those UAS operators who receive waivers. Under Part 107 waivers, UAS operators may apply for a waiver to operate the UAS by completing an online application that requires information on how the operator intends to safely conduct the operation. *Read more*

PRIVACY TIP #83

"Alexa, Disconnect Yourself from the Internet Now!" BrickerBot Malware Attacking IoT

We often talk about how anything that is connected to the Internet is

hackable and unsafe, as well as how to be careful when you buy and connect devices, products, appliances, home security systems and other wireless “things.” These are called the Internet of Things, or “IoT.” Alexa is an IoT “thing.”

Cybersecurity literature constantly warns us about vulnerabilities to IoT. The newest vulnerability is called BrickerBot. BrickerBot is malware that is targeting insecure IoT devices.

Without getting too techy, basically, the BrickerBot malware forms a Permanent Denial-of-Service (PDOS) botnet. What the heck does that mean? It means that when it gets into the IoT insecure device, it is able to destroy basic device functions and corrupt its storage, disrupt internet connectivity, mess up its performance, and wipe all of the files on the device. The purpose seems to be to destroy usage of the device, as opposed to gaining access to information on the device to exfiltrate it and sell it.

So the tip of the week is to continue to patch all devices, including IoT devices, secure all IoT “things,” and think and think again about why you really need that IoT thing. Assess the information it is collecting, storing, transmitting and now—losing, before you buy it and connect it. I wonder if Alexa can actually disconnect herself in the face of BrickerBot? More on Alexa next week…