Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

World Energy Council Issues New Report on Cyber Risk

Because cyber risk presents a "unique concern" in the energy sector, the World Energy Council has issued a new report entitled "The Road to Resilience: Managing Cyber risks" to its industry leaders. Referring to two cyber-attacks that affected the nuclear industry in the past few years—an attack by "Slammer" in the U.S. in 2003, and a hacking in South Korea in 2014-2015, the report states that "[L]arge centralised infrastructures are especially at risk due to the potential 'domino effect' damage that an attack on a nuclear, coal, or oil plant could cause." *Read more*

Draft Cybersecurity Self-Assessment Tool Published

The National Institute of Standards and Technology (NIST) recently published a draft cybersecurity self-assessment tool entitled "The Baldrige Cybersecurity Excellence Builder," which provides organizations with a tool to determine its security maturity level. *Read more*

NIST Extends Deadline for Comments to Mobile Device Infrastructure Guidance

All enterprises are struggling with the security risks posed by the use of mobile devices by employees. Companies want their employees to have easy access to information so that they can perform their job functions in an efficient and easy way, yet allowing easy access to company data through mobile devices are security professionals' nightmare. In response, the National Institute of Standards and Technology (NIST) has issued guidance entitled "Assessing Threats to Mobile Devices & Infrastructure: The Mobile Threat Catalogue." *Read more*

October 13, 2016

FEATURED AUTHORS:

Linn Foster Freedman
Kathryn M. Rattigan
Pamela H. Del Negro
Benjamin C. Jensen

FEATURED TOPICS:

Cybersecurity
HIPAA
Enforcement + Litigation
Data Privacy
Data Breach
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

HIPAA

OCR Releases HIPAA Guidance on Cloud Computing

On October 6, 2016, the Department of Health and Human Services Office for Civil Rights (OCR) released HIPAA guidance on cloud computing (Guidance). The Guidance is intended to help covered entities and business associates understand their HIPAA obligations in cloud computing arrangements, and clarify the HIPAA obligations of cloud service providers (CSPs). *Read more*

ENFORCEMENT + LITIGATION

16 Data Breach Class Action Lawsuits Filed Against 21st Century Oncology Consolidated

We previously reported that 21st Century Oncology suffered a data breach in October 2015. As a result of the data breach, sixteen class action cases were filed against the cancer treatment provider in Florida and California. These suits allege various causes of action, but include violation of the Fair Credit Reporting Act, the Florida Deceptive and Unfair Trade Practices Act, and delay in providing notification to the patients, since the breach occurred in October 2015, 21st Century was alerted to the intrusion by the FBI on November 13, 2015, and patients weren't notified until March 4, 2016. *Read more*

DATA PRIVACY

FCC Releases Proposal for New Privacy Rules Governing ISPs

In an October 6th blog post and accompanying fact sheet, FCC Chairman Tom Wheeler outlined his proposal for new privacy rules governing Internet Service Providers (ISPs) to be considered by the full Commission during its upcoming monthly meeting on October 27th. Chairman Wheeler's post detailed the scope of the issue – ISPs are collecting information based on millions of customers' online activity and there are currently no rules in place governing how ISPs are permitted to use and share its customers' personal information. *Read more*

Massachusetts DOT Seeks to Retain Driver Data from the State Turnpike

The Massachusetts' State Department of Transportation (MassDOT) has proposed a policy by which it would retain drivers' speed data for

30 days after it is collected on the Massachusetts Turnpike through its new all-electronic toll stations.

MassDOT explains that the speed data must be collected in order to synchronize the new tolling system's cameras so that the systems can accurately take photographs of vehicles' license plates as they drive through the new tolls. However, privacy advocates have raised some concerns. *Read more*

DATA BREACH

Surgeon General Notifies Employees of Breach

According to the surgeon general of the United States, the personal information of current, former, and retired employees of the United States Public Health Service Commissioned Corps and their dependents has been compromised. These 6,600 individuals are employed to provide medical services to underserved populations and to assist with disease control, and the safety of drugs and medical devices, and include physicians, surgeons, pharmacists, dentists, nurses, and therapists. *Read more*

Central Ohio Urology Group Notifies 300,000 Patients of Breach

Approximately 300,000 patients of Central Ohio Urology Group have been notified that their protected health information has been stolen and posted online. The data included 401,828 files that included videos, images, texts files, spreadsheets, and other documents. *Read more*

PRIVACY TIP #56

Be Careful before You Link Your Home Appliance to Your Smartphone, and Change Your Passwords Now

Last week, Brian Krebs reported that hackers using a malware dubbed "Marai" have identified hundreds of thousands of home and office devices that have weak security. Then, the hackers released the malware publicly so anyone can use it and intrude into home and office devices that do not have proper security to thwart the attack through a distributed denial of service (DDos) attack. The hackers can gain access to these devices and turn them off, disrupt the way they work, or use the control of the device to extort money from the homeowner.

It is reported that there are over 23 billion devices on the market today that are connected to the Internet of Things (IoT), and that number is growing rapidly. The IoT includes anything connected to

the Internet, but for my purpose today, it means your home security system, oven, TV, baby monitor, routers, DVDs, window lock systems, refrigerators, pet collars, and toys.

It is easy for the hackers to gain access to your baby monitor because when the baby monitor was developed data security was not the priority. No one was thinking that hackers could or would want to hack into a baby monitor.

The bigger problem is when a home is thoroughly connected to the Internet, including all of its appliances. According to Alfred Chung of *Guidance Software*, "Anyone with access to a fully connected home can build a detailed profile about the occupants…They can gather data about the time of day when the home is occupied, the number of people inside the home at various times, personal details like age, appearance, and gender of those living in the home…With connected appliances, they can even tell what food occupants store in their fridge…"

Although hackers would be very disappointed with the food I store in my fridge, it is still very creepy and scary to think that all of this information can be obtained because my home is a connected home. Of course, you all know that I would never connect my fridge, my security system, or my TV to the Internet, so this should not affect me. However, I know many of you do love to connect your appliances to your phone, so before you connect that appliance, think twice—do you really need to connect that device to the internet?

Finally, because of the massive attacks that have occurred recently, as reported by Krebs, it is being widely suggested that, if your home and its appliances are IoT and connected, change your passwords immediately.