Attorney Advertising

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

Power Company Fined for Contractor Copying Data to its Own Insecure Network

Vendor management continues to be a problem for all industries, but some are scarier than others. The North American Electric Reliability Corp. (NERC) recently provided notice to the Federal Energy Regulatory Commission that an unidentified power company has reached a settlement with the Western Electricity Coordinating Council for $2.7 million to resolve two violations of NERC's critical infrastructure protection standards. *Read more*

Energy Sector: Hit Hard and Worried

One only needs to read the headlines to understand that critical infrastructure in the U.S., including the energy sector, is an obvious target for malicious individuals. According to a new report by Marsh, entitled "Could Energy Industry Dynamics be Creating an Impending Cyber Storm?", more than one in four respondents of an energy sector survey admitted that their company had been hit by a damaging cyber-attack in the last year. Additionally, more than 75 percent of the respondents admitted they are worried that a cyber-attack would interrupt business operations in the future. Despite the worry, half of the executives surveyed were unable to quantify or envision what the worst exposure would be to the company from a cyber-attack. *Read more*

NIST Issues Energy Sector Asset Management Project

According to the National Institute of Standards and Technology (NIST), the energy sector relies on industrial control systems assets to "generate, transmit, and distribute power, and to drill, produce, refine, and transport oil and natural gas." These industrial control systems include supervisory control and data acquisition (SCADA) systems, distributed control systems, programmable logic controllers, and intelligent electronic devices that control operational technology networks. These systems are targets of cyber-attacks according to NIST. A successful cyber-attack against these industrial control

March 29, 2018

FEATURED AUTHORS:

Conor O. Duffy
Linn Foster Freedman
Kathleen M. Porter
Kathryn M. Rattigan

FEATURED TOPICS:

Autonomous Vehicles
Cybersecurity
Data Breach
Drones
Enforcement + Litigation
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

systems could “cause disruptions to the power grid and to oil and gas assets and processes.” Needless to say, such disruptions would cause chaos. *Read more*

DATA BREACH

Oregon Strengthens Data Breach Reporting Law

Oregon Governor Kate Brown recently signed a new data breach reporting law (S. 1551) that toughens the state’s existing requirements.

The new requirements include that companies are required to notify individuals within 45 days after a data breach has been discovered, unless a delay in notification is requested by law enforcement. It expands the definition of personal information to include passport information, biometric information, any information that would permit access to a consumer’s financial account, health insurance account number, and a consumer’s medical history, mental or physical condition, or a diagnosis by a medical provider. *Read more*

ENFORCEMENT + LITIGATION

Congress Enacts CLOUD Act within Omnibus Spending Bill to Address Overseas Storage of Electronic Data, Potentially Mooting Supreme Court’s Pending *Microsoft* Case

On March 23, 2018, the President signed into law the Consolidated Appropriations Act of 2018 (H.R. 1625), an omnibus spending bill that includes the Clarifying Lawful Overseas Use of Data Act (the CLOUD Act). Among other provisions, the CLOUD Act amends the Stored Communications Act of 1986 (18 U.S.C. §§ 2701-2712, hereinafter the SCA) by adding a new § 2713. *Read more*

DRONES

FAA Issues Refresher on Part 107 Rules

Last Friday, the Federal Aviation Administration (FAA) released a “refresher” on its Part 107 rule for small unmanned aircraft systems (UAS or drones) in a “Fact Sheet” available here. The Fact Sheet outlines all the basics of Part 107. *Read more*

New Study Estimates Half of Drone Flights Will be Autonomous by 2022

A new study was released last week by consulting firm Frost & Sullivan, which estimates that more than half of the global commercial unmanned aircraft system (UAS or drone) flights will be conducted autonomously by the year 2022. The study says these autonomous flights will function "much like warehouse robots operate today." Frost & Sullivan's research director, Michael Blades, said that "the UAS market is becoming an ecosystem focused on information and value-added services, where the drone is a tool acting as a cog in the big data machine." Accordingly, the study predicts that success in the UAS ecosystem will likely be achieved by companies that can safely, quickly, and inexpensively offer high-level data for real-time decision-making. Another interesting prediction by this study is that by 2022, the UAS industry will mimic the cell phone industry, with few hardware providers and a myriad of open-source and sensor providers for specific applications. *Read more*

Virginia Passes Drone Trespassing Bill

Virginia H.B. 638 (the Bill), which concerns unmanned aircraft systems (UAS or drones), passed the Virginia House and Senate and is now awaiting signature from the governor. The Bill "prohibits any person, after being given actual notice to desist, from knowingly and intentionally causing any UAS to enter the property of another and come within 50 feet of a dwelling house with the specific intent to coerce, intimidate, or harass any other person." The Bill also prohibits registered sex offenders from "using or operating a UAS to knowingly and intentionally follow, contact or capture images of another person without permission of such person when images render the person recognizable by his face, likeness or other distinguishing characteristic." It also prohibits the respondent of a protective order from using UAS in the same way. A violation could result in a misdemeanor, which includes a sentence of up to 12 months in prison. *Read more*

Drone Delivery Canada's Newest UAS to Carry 400 Pounds

Drone Delivery Canada (DDC) began development of its newest drone, the Condor, last week, which is being engineered to provide payload capacities of up to 400 pounds. The Condor will be able to accept pallet-sized payload shipments (for transporting bulk cargo—both in Canada and abroad) and fly approximately 93 miles. Most important, the Condor will be fully integrated with DDC's proprietary FLYTE management system, which has been extensively tested in Canada and also recently tested in the United States at Griffiss International Airport in Rome, New York. CEO of DDC, Tony Di Benedetto, said, "Our engineering team is focused on building out our

fleet to provide drones capable of addressing a wide range of client requirements in different geographies. The Condor will be our first delivery drone that offers our customers a platform for greater capacities of bulk shipments." DDC will start testing its Condor drone late in 2018. *Read more*

Walmart's Patent for Drone Customer Service

Walmart recently filed a patent for drones to aid shoppers inside their stores. Shoppers would use a mobile device, provided by the store, to request a drone, and then direct the drone to conduct a price verification of a product or to guide the customer to a particular product through the use of a visual projection or audio output. *Read more*

AUTONOMOUS VEHICLES

Snowy Conditions: Yandex Releases Video of Self-Driving Car

Russian company, Yandex (often compared to Google here in the United States), recently debuted its very own self-driving car. Last week, Yandex released a video depicting its self-driving car driving through snowy streets of Moscow–an extraordinary feat navigating inclement weather and adverse driving conditions. The video shows a driver with his hands in his lap as the car turns its own wheel to navigate around snowy embankments and carelessly parked cars. Yandex combined cameras, radar, lidar, and specialized satellite navigation. While this is only the beginning of its prototype and its technology, Yandex hopes to create a universally applicable technology for cars all around the world. Dmitriy Polischuk, head of Yandex, said, "With enough data, everything that can be identified by human eyes can also be identified by a computer with proper technologies." *Read more*

PRIVACY TIP #132

Social Security Fraud

As our readers know, I am particularly interested in protecting our seniors from fraud. They continue to be a vulnerable population and unfortunately, here is another scam that makes me mad: Social Security fraud.

Many elect to have their Social Security payments deposited by direct deposit, and in fact, it is required by the Social Security Administration (SSA). SSA has an online portal management system that recipients

can check, much like an online banking account, to confirm that their payments have been deposited into their account.

Individuals have been advised to register for the online portal whether they receive benefits or not, as there is a rise in cases where identity thieves are registering in your name without your knowledge before you do and then diverting your funds into their bank account.

The scam works like this: the fraudster goes to the online portal and uses your personal information and requests that the social security benefits be diverted to prepaid debit cards or green dot cards. It is very similar to what we have seen repeatedly with fraudulent tax returns being filed in individuals' names and a tax refund being provided in the form of a prepaid debit card. Unfortunately, the fraudsters can also register by phone by giving SSA your name, birthdate, place of birth, address, mother's maiden name, and telephone number. Most of this information is easily accessible online and is not tricky.

In some cases, when someone signs you up for social security benefits or payments, a letter will be sent in the mail to confirm the enrollment. But if the fraudster changes your address, you may never know this has happened unless you check the portal frequently.

More than 34 million people in the U.S. interact with the SSA through the online portal. The SSA's Office of Inspector General found that between February 2013 and February 2016, 30,000 suspicious MySSA registrations occurred and over 58,000 allegations of fraud related to MySSA accounts were reported.

If you already receive Social Security benefits, check your online account frequently, as you would your online banking account. Check all of the information carefully, including your demographic information to make sure it hasn't been changed or altered even slightly. If you are close to receiving benefits, consider signing up now so no one else can sign up in your name.

Finally, if you have been the victim of a data breach and are considering placing a credit freeze on your credit accounts with the four credit bureaus, you may wish to consider activating your MySSA online account before you activate the credit freeze, as you will not be able to activate the MySSA account once you activate a credit freeze with the credit bureaus. The good news is that if you have already implemented a credit freeze, it appears that a fraudster will not be able to open your MySSA account either. For questions or concerns, call SSA's toll free number at 1-800-772-1213.