Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

NCCoE Releases Guidance for Securing Manufacturing Industrial Control Systems

The National Cybersecurity Center of Excellence (NCCoE) has released "Capabilities Assessment for Securing Manufacturing Industrial Control Systems," a draft Project Description for the manufacturing sector. The goal of the guidance is "to provide industry with detailed information to establish an anomaly detection and prevention capability in their own environments." This first document is the first of a four-part series and addresses only behavioral anomaly detection capabilities. *Read more*

Tesco Bank Cyber-Robbery—Some Implications for U.S. Banks—andTtheir Depositors

UK-based Tesco Bank froze online transactions on Monday after discovering that cybercriminals stole money from 20,000 different customer accounts. The exact method used by the perpetrators is still under review, but preliminary analysis suggests the attackers exploited weaknesses in the bank's online payment system related to the processing of debit card transactions. With the prospect that similar attacks may occur in the United States, U.S. financial institutions and their customers should be asking, "Who foots the bill when cybercriminals make off with a customer's money?" *Read more*

NIST Releases Craft NICE Cybersecurity Workforce Framework

There is a dearth of cybersecurity talent in the U.S., and it is one of the fastest-growing fields for job opportunities. Because cybersecurity is still a developing field, there are different definitions of jobs and roles that are not consistently applied across industries and organizations. To help decipher those differences, the National Institute of Standards and Technology (NIST) has developed a resource for U.S. employers, which is basically a dictionary that will help organizations define roles, and "share information in a detailed, consistent and descriptive way." *Read more*

November 10, 2016

FEATURED AUTHORS:

Scott M. Baird
Linn Foster Freedman
Kathryn M. Rattigan
Norman H. Roos

FEATURED TOPICS:

Cybersecurity
Data Privacy
HIPAA
Drones
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

HIPAA

Three Former Warner Chilcott District Managers Prosecuted for HIPAA Violations

The United States Attorney's Office for the District of Massachusetts recently announced that three former district managers of the pharmaceutical firm Warner Chilcott have been sentenced for violating the Health Insurance Portability and Accountability Act (HIPAA) and committing health care fraud. *Read more*

DRONES

Night Ops Top-Requested Part 107 FAA Waivers

At a recent Commercial Unmanned Aerial Vehicles (UAV) Expo in Las Vegas, Nevada, a Federal Aviation Administration's (FAA) attorney, Dean Griffiths, explained that the top three requests for Part 107 commercial drone operations waivers were for night operations, operations over people, and flight beyond the visual line of sight. *Read more*

Will Uber Ever Hit the Skies?

While Uber has been trying to pioneer self-driving technology, debuting its first self-driving taxis in Pittsburgh, Pennsylvania, last month, Uber is now looking at "vertical take off and landing" (VTOL) technology. *Read more*

DATA PRIVACY

As Smart Cities Emerge, "Smart" Policies Must Come Too

Many American cities are already adopting technologies to improve urban living—bike share systems, street parking payment through smart phones, and paying tolls through E-ZPass. However, with these so-called "smart cities" and increased efficiency comes some risks to individual citizens that many policymakers have not yet considered. *Read more*

PRIVACY TIP #60

Cybersecurity Tips for the New Administration

It is hard to stay focused after election night.

Because the new administration has a dearth of plans, here are some tips for it to get a jump start on cybersecurity priorities, including the following:

- help U.S. companies combat hacking by foreign governments, including through investigative and diplomatic efforts (and, yes, that includes Russia);
- provide a centralized and sophisticated platform for public-private sharing of cyber intrusions, along with rapid response and assistance to stop the heist of U.S. companies' intellectual property and personal data and to prevent other companies from becoming victims;
- implement better practices around the protection of U.S. government employee data, as well as citizens' data, including the IRS;
- accelerate the implementation of the Privacy Shield to help companies compete in the global economy;
- promote educational programs from K-12 to address the present dearth of cybersecurity talent in the U.S.;
- increase resources to prosecute hackers and criminals and bring them to justice as a deterrent; and
- educate members of Congress on the risks to assure appropriate resources are devoted to protecting data to prevent a cyber war.

Cybersecurity should be a top priority for the new administration. Whether it will be remains to be seen.