Attorney Advertising

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

McAfee Report Lists Health Care Sector as Most Targeted Industry for Cyber-Attacks

In its cybersecurity incident report outlining vulnerabilities for the second quarter of 2017, security firm McAfee lists the health care sector as having suffered the most security incidents, which surpasses the public sector for the first time in six quarters. It confirmed that cyber-attacks against the health care sector continue to increase.

Although that statistic is disturbing, but not surprising, alarming statistics from the report include that there was a 67 percent increase in new malware samples in the second quarter of 2017, which equates to a whopping 52 million different kinds of malware in that quarter alone. The total number of malware samples were up 23 percent to almost 723 million different types of malware. *Read more*

U.S. Treasury Warns Financial Institutions of Venezuelan Corruption and Money Laundering

The Financial Crimes Enforcement Network (FinCEN) of the U.S. Department of the Treasury issued an advisory on September 20 warning U.S. financial institutions of "money laundering schemes used by corrupt Venezuelan officials." The advisory was addressed to private banking units, chief risk officers, chief compliance officers, AML/BSA analysts, sanctions analysts, and bank legal departments and identified a number of red flags to help financial institutions spot instances where corrupt senior politicians may be attempting to use Venezuelan government contracts to embezzle funds and receive bribes. *Read more*

DATA BREACH

Home Depot Settles Data Breach Class Action Case with Financial Institutions and Counsel for $42.55 million

October 5, 2017

FEATURED AUTHORS:

Scott M. Baird
Linn Foster Freedman
Joanne J. Rapuano
Kathryn M. Rattigan
Matthew P. Rizzini
Norman H. Roos

FEATURED TOPICS:

Cybersecurity
Data Breach
Data Export Control
Drones
Health Information
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

Following its data breach in 2014, Home Depot was sued by thousands of financial institutions requesting recovery of costs associated with the issuance of new credit and debit cards to 50 million individuals affected by the breach. Last week, an Alabama federal judge approved a proposed settlement with the financial institutions for $27.25 million. The judge also approved a request for $15.3 million in attorneys' fees for the attorneys representing the financial institutions in the class action case. *Read more*

Sonic Latest Food Chain to Suffer Credit Card Breach

After being notified of "unusual activity" on credit cards by its credit card processor, Sonic Drive-In has confirmed it is working with forensic experts and law enforcement on a potential credit card breach. It has not been reported whether debit cards may be involved as well. *Read more*

DATA EXPORT CONTROL

To Be Cyber Secure May Not Mean You Are Export Secure

Even though an environment is secure by cybersecurity standards, it may not be “export” compliant. Ensuring that technical data is compliant with both export regulations and cybersecurity requires an understanding of what export-controlled technical data/technology relate to and how they work together. The two major export control regulations, the International Traffic In Arms Regulations (ITAR) and the Export Administration Regulations (EAR), define controlled technical data/technology differently.

An effective approach requires incorporating export regulations into cybersecurity protocols. This means the IT architecture needs not only to embrace the encryption requirements and authentication protocols to access a company’s systems, files, and share drives but also to analyze what employees have access to once they have validly entered their companies' domain. *Read more*

HEALTH INFORMATION

Study Finds 73 Percent of Medical Professional Use Other People's Passwords

We all know by now that we are not supposed to give our passwords to anyone else or use someone else's passwords to access an electronic system. Despite this basic data security tenant, a new study by Healthcare Informatics Research reports that 73 percent of

medical professionals admit they have used another person's password to access an electronic medical record (EMR).

The survey asked 299 medical professionals in hospital settings if they had ever used someone else's password to access an EMR. Of those questioned, 100 percent of the medical residents said, they had, and 57.7 percent of nurses also admitted they had.

The study found that the reason the residents had violated basic security hygiene was that they had not been given a user account of their own or did not have access rights to information that was needed to fulfill their duties. *Read more*

DRONES

BZZZ! Research on the Annoying Noise of UAS

The National Aeronautics and Space Administration (NASA) released the results of a study that determined how annoying the bzzz of unmanned aircraft systems (UAS or drones) really is to the public on the ground below. NASA researchers compared the noise generated by drones to that of cars and found that indeed, the public at large was more annoyed with drone noise than with car noise. The report, "Initial Investigation into the Psychoacoustic Properties of Small Unmanned Aerial System Noise," not only deals with more than just the annoyance level of drone noise, but also analyzes the effects on the environment around the drone. *Read more*

Drone Use Prohibited at DOI Landmarks

The Federal Aviation Administration (FAA) has prohibited drone flights at 10 Department of the Interior (DOI) landmarks across the country. Title 14 of the Code of Federal Regulations (14 CFR) § 99.7 – "Special Security Instructions" is being used by the FAA to address concerns about drone use at the 10 sites. *Read more*

PRIVACY TIP #108

October Is National Cybersecurity Awareness Month: Beware of Scam Netflix Email

Happy National Cybersecurity Awareness Month. I wish it were more uplifting than the current state of affairs, but it has never been so important.

Impersonating Netflix is one of the most recent scams to hit

consumers.

If you are a Netflix user, beware of a new scam that looks like an email that comes from Netflix that tells users that their account is disabled and asks users to input bank account information to enable the account. It uses the Netflix logo and looks very real. It says that Netflix is having “trouble with your current billing information” and will try later, but in the meantime, please provide current information like telephone number and bank information.

When users input the information, the hackers now have access to their bank information.

The email is sent to users from supportnetflix@checkinformation.com. Wen users click the embedded link within the body of the email, it forwards them to a fraudulent Netflix page where they enter their bank information, which hackers then have access to and can use.

Don’t relay your bank account information through a website or online and beware of this scam using Netflix’s logo. Enjoy your movies—but always be safe with your bank account information.