Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

$64 Million in Bitcoin Stolen from NiceHash

Many are lamenting not purchasing bitcoin now that its value has skyrocketed. Yesterday, Massachusetts Secretary of State William Galvin warned investors to stay away from investing in bitcoin, as he considers it a financial bubble that is a gamble for investors. He stated, "It's simply a creation of a vehicle which doesn't exist backed by any government, there's no entity that supports it, so if it collapses, it's gone….It's just not a good idea."

Last week, cryptocurrency marketplace NiceHash announced that it suffered a security breach when an intruder was able to access its payment system through a "sophisticated social engineering" attack and whisked away the contents of its bitcoin wallet, which contained 4,700 bitcoins. The estimated value of those 4,700 bitcoins? $64 million. $64 million gone in a flash. *Read more*

Russian Hackers: Desperate for U.S. Information

The latest report [see related post] regarding Russia stealing U.S. cyber secrets is yet again centered around the National Security Agency (NSA) using contractors to gain access, in some cases, to classified data.

It has been reported that an NSA contractor (fired back in 2015) put highly classified U.S. cyber secrets on his home computer, which included information on how to infiltrate foreign computer networks and protect against cyber-attacks. As reported by *The Washington Post* (10.05.2017), the Russian government-backed hackers were able to identify the files through the contractor's use of the antivirus software Kaspersky Lab, a Russian-based company. Ironically, the employee had worked at the NSA's Tailored Access Operations unit for elite hackers. Kaspersky Lab is a company whose products were banned from U.S. government networks because of suspicions they help the Kremlin conduct espionage. *Read more*

December 14, 2017

FEATURED AUTHORS:

Pamela H. Del Negro
Linn Foster Freedman
Joanne J. Rapuano
Kathryn M. Rattigan

FEATURED TOPICS:

Cybersecurity
Data Breach
Drones
HIPAA
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

DATA BREACH

PayPal's Canadian Payments Processing Company Suffers Breach

PayPal has acknowledged that TIO, the Canadian payments processing company that it acquired in July 2017, has suffered a data breach that compromised the information of up to 1.6 million users. TIO processes utility and other bill payments and has over 60,000 kiosks in North America.

PayPal suspended TIO's operations in November, as it "did not adhere to PayPal's information security standards." PayPal has confirmed that the breach did not affect its network and that TIO's system is separate from PayPal's system. According to PayPal, TIO is in the process of notifying affected individuals and is offering free credit monitoring for those individuals. *Read more*

Henry Ford Health System Notifies 18,000-Plus Patients of Health Data Breach

On December 6, 2017, Henry Ford Health System (HFHS) disclosed that health information of 18,470 patients may have been viewed or stolen. HFHS became aware of the incident on October 3, 2017, after employee credentials were accessed or stolen. According to a statement published on HFHS's website, Social Security numbers and credit card information were not revealed. Affected information may include a patient's name, date of birth, date of service, medical record number, provider name, department name, location, and health insurer. HFHS has stated that it will issue new medical record numbers to patients upon request. *Read more*

HIPAA

OCR Warns Healthcare Industry of Risks with Previous Employees

In its November newsletter, the Office for Civil Rights (OCR) made a great point that we are seeing in the industry—the risks associated with previous employees. According to its newsletter, entitled "Insider Threats and Termination Procedures," the OCR states, "Data breaches caused by current and former workforce members are a recurring issue across many industries, including the healthcare industry." We can confirm this is true.

The OCR further states that when an employee is terminated or quits, "it is extremely important that covered entities and business associates prevent unauthorized access to protected health

information (PHI)…" The OCR provides tips for healthcare entities to prevent unauthorized access to PHI by former employees. *Read more*

DRONES

The City-Scale Impacts of Drone Delivery Report

A report developed by the RAND Corporation, a research organization that develops solutions to public policy challenges, called, "What's the Buzz? The City-Scale Impacts of Drone Delivery," which deals with city package deliveries using drones. The research used mathematical models to assess the impact of drone deliveries on energy consumption, infrastructure requirements, aerial congestion, privacy, and noise. It did not however, address, how weather could affect drone delivery logistics, but the logistics industry has a lot more immediate challenges to overcome before getting to the issue of weather. *Read more*

PRIVACY TIP #118

How to Avoid "Credential Stuffing"

'Tis the season of stuffing stockings. 'Tis also the season of "credential stuffing." What is credential stuffing you ask?

According to Wikipedia, "credential stuffing is a type of cyber-attack where stolen account credentials are used to access user accounts through large-scale automated login requests directed against a web application."

According to Shape Security, credential stuffing is "The #1 Cause of Account Takeover."

Credential stuffing is conducted by cybercriminals who have obtained access to individuals' usernames and passwords and can then access online platforms using those stolen user names and passwords. Usernames and passwords are commonly referred to as "credentials." Your "credentials"—are the username and password that you use to get onto an online platform to shop, conduct online banking, and access frequent flyer miles, or bitcoin accounts, etc. If the username and password are validated, anyone can access those accounts.

Cybercriminals have developed sophisticated ways to use technology, through automation, to test usernames and passwords, and when successful, to take over individuals' accounts. Once they can take over the account, they have access to and can steal whatever is in it. It is estimated that over the past three years, $2.3 billion has been lost to account takeover.

The reason why credential stuffing is so successful for these cyber criminals is because people use the same passwords over and over. It is difficult to remember so many different passwords for each online activity. An effective way to prevent becoming a victim of credential stuffing is to not use the same password across online platforms, to change passwords frequently, and to use multifactor authentication for online activity.

So enjoy stuffing those stockings this holiday season but don't become the victim of credential stuffing.