Attorney Advertising

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

Cisco Warns of VPN Bug

Cisco is warning customers using its Adaptive Security Appliance (ASA) software about a virtual private network (VPN) bug that could "allow an unauthenticated, remote attacker to cause a reload of the affected system or to remotely execute code" and "allow an attacker to take full control of the system." *Read more*

HIPAA

Fresenius Pays OCR $3.5M for Five Separate Data Breaches Affecting a Total of 521 Individuals

In the first settlement for HIPAA violations in 2018, Fresenius Medical Care North America (Fresenius) has agreed to pay $3.5 million to the Office for Civil Rights (OCR) to settle allegations against it relating to five data breaches that occurred over a four month period in 2012. Interestingly, the five separate breaches affected the information of 521 individuals, making some question whether the punishment fits the crime. *Read more*

ENFORCEMENT + LITIGATION

United States Supreme Court Considers Whether to Weigh in on Circuit Split in Data Breach Actions

In October 2017, a healthcare insurer, CareFirst, petitioned the United States Supreme Court, requesting the Court to clarify the constitutional standing requirement for plaintiffs seeking to bring claims regarding their exposure during corporate data breaches.

In order to invoke federal court jurisdiction, a plaintiff must plead an actual or imminent injury. The Supreme Court has held that the imminence requirement is satisfied where a threatened injury is "certainly impending" or there is "substantial risk" that future harm will occur. However, where the injury requires a chain of inferences in order to find harm or speculation regarding actors not before the court, an injury is not "imminent" and there is no standing. *Read more*

DATA BREACH

Massachusetts AG Launching Online Data Breach Reporting

February 8, 2018

FEATURED AUTHORS:

Linn Foster Freedman
Kathryn M. Rattigan
Carrie C. Turner

FEATURED TOPICS:

Cybersecurity
Data Breach
Drones
Enforcement + Litigation
HIPAA
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

Portal

Massachusetts Attorney General Maura Healey recently announced that her office will be launching a new online data breach reporting portal for companies to use to report data breaches to her office pursuant to the Massachusetts data breach notification statute.

The use of the portal is voluntary and does not relieve companies of their statutory obligations, including notifying the Massachusetts Office of Consumer Affairs and Business Regulation (which has changed its location and address). *Read more*

DRONES

Validity of Ball State University Drone Policy Questioned

Chad Budreau, Public Relations and Government Affairs Director of the Academy of Model Aeronautics, says that Ball State University's (Ball State) "Policy for the Use of Unmanned Aircraft Systems (Drones)" violates the Federal Aviation Administration's (FAA) small unmanned aircraft systems rule (Part 107). The Ball State policy, issued back in November 2017, states that all drone operators must request approval from the Ball State Office of Risk Management (ORC) before flying a drone on the Ball State campus at least 14 days prior to the flight. The policy also states that all drone operators must wear an operator's badge, which will be issued by the ORC. *Read more*

Drone Detection Technology at the Waste Management Phoenix Open

This past weekend, Scottsdale, Arizona police used new drone detection technology at the Waste Management Phoenix Open to keep both attendees and players safe. Sergeant Ben Hoster said, "Drones are becoming so inexpensive and so popular, we are getting ahead of this technology," by linking up with Dedrone (an anti-drone solutions company) and Aerial Armor (a security solutions for drone intrusions business). The Scottsdale police use a device that is nothing more than a box with antennas to detect when a drone pops up. The device detects the drones usage and a message is sent to officers in the area to look for the drone and find the operator. The data collected by the device is analyzed by software, which then sends out an alert to officers (or security staff at an event like the Waste Management Phoenix Open) of the unauthorized drone. *Read more*

North Carolina Seeks to Deliver Emergency Supplies via Drone

The North Carolina Department of Transportation (DOT) and state officials are currently building plans to use drones to deliver emergency supplies across the state; however, several hurdles need to be overcome first. Basil Yap, program manager of the Unmanned Aircraft Systems of the North Carolina Division of Aviation, says, "How do drones safely fly beyond visual line of sight, when you can't see the drone flying? You'll need to be able to detect other aircraft in that airspace. Another concern is: 'How do these drones

communicate securely when flying beyond our line of sight?' And that would be utilizing technology like cellular technology, or maybe even satellite technology." *Read more*

PRIVACY TIP #125

Check + Set LinkedIn Privacy Settings

It is well known that hackers and fraudsters surf Facebook to find individuals who have not protected their information through Facebook's privacy settings. People put a lot of information on Facebook that is very personal and can give criminals detailed leads on how to launch successful campaigns against unsuspecting victims.

Less publicized is the fact that these same criminal surfers are also looking at individuals' LinkedIn profiles to gain information about the individual and its employer to launch successful phishing campaigns.

Through LinkedIn, cybercriminals easily find out who individuals are employed by, and then use the "see all employee" feature to identify coworkers. This provides the hackers with a list to start sending targeted phishing emails.

They can assemble all of the information from the company's LinkedIn connections, and figure out the company's suppliers, technology vendors and third party service providers, such as payroll, HR and benefits providers and customer relations management platform. This provides them with trusted sources to use for phishing campaigns.

According to the German Ministry of Interior, social media sites such as LinkedIn have been used by Chinese intelligence personnel for espionage. It found that these intelligence personnel created fake profiles of HR specialists, head hunters, recruiting specialists, and project leads to reach out to potential targets to compromise individuals and companies.

The study in Germany reminds us to review and set LinkedIn privacy settings. To start, go to your LinkedIn account, click on your picture and click on Privacy and Settings in the drop down menu and go through each section to make sure it is set in the manner you wish.

For step-by-step instructions, CyberScout has published an easy to follow guide, which can be accessed here.