Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

Old Locky Ransomware Resurfacing Using PDFs—Alert Your Employees

We have previously reported on the vicious ransomware Locky and how it victimized companies throughout 2016 [View previous posts here, here, and here]. Although Locky quieted down in late 2016, according to researchers at Cisco Talos, Locky is perking up again in 2017 in a major way. Only this time, instead of using phishing email schemes that used attached Word documents, the attackers are now using PDF files. When the user opens the PDF, the PDF contains an embedded Word document, which the user is asked to open. When the user opens the Word document, the user is told that the document is protected and that macros need to be enabled to view the document. When the macros are installed by the user, the ransomware is downloaded. *Read more*

DATA BREACH

Verizon 2017 Data Breach Investigation Report Released

We follow the Verizon Data Breach Investigation Report each year. It just hit the newsstand and, as always, is full of insights. The report collected data from 65 organizations in 84 countries, including 42,068 cybersecurity incidents and 1,935 data breaches. The major themes of the report are that no one thinks it's going to be them, until it is; organizations think they've got the basics covered; people are also still failing to set strong passwords; and people rely on how they've always done things. *Read more*

New Mexico Enacts Data Breach Notification Law

Governor Susana Martinez recently signed into law the New Mexico Data Breach Notification Act (the Act), making New Mexico the 48th state (plus Puerto Rico and the District of Columbia) to adopt legislation mandating the provision of notice in the event of a data

May 4, 2017

FEATURED AUTHORS:

Conor O. Duffy
Linn Foster Freedman
Sean Lawless
Kathryn M. Rattigan

FEATURED TOPICS:

Cybersecurity
Data Breach
Data Privacy
Drones
Enforcement + Litigation
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

breach. *Read more*

DarkOverlord Allegedly Hits Netflix and Releases *Orange Is The New Black* Episodes

We have previously reported about the activities of The DarkOverlord [view related post]. It is now being reported that a hacker and/or hacking group known as The DarkOverlord announced on Twitter over the weekend that it has absconded with 10 episodes of Netflix's *Orange Is The New Black* series and has released several upcoming episodes to an illegal file-sharing service. *Read more*

Hacker Hits HipChat—Reset Passwords

An unknown intruder was able to access team communication platform HipChat last weekend, allowing access to the account information of users, including email addresses, hashed passwords. and names. There is also a chance that actual room metadata, which includes the room name and room topic, may have been compromised. The cyber-attacker was able to access a server in the HipChat Cloud web tier. *Read more*

ENFORCEMENT + LITIGATION

Home Depot Agrees to Settle Data Breach Shareholders' Suit

In a surprise move late last week, Home Depot has agreed to settle a shareholders derivative suit filed against current and former members of the Board of Directors and the chief executive officer and chief information officer (CIO) following a massive data breach that occurred in 2014. The shareholders allege that former and current board members breached their duty of loyalty to the company by failing to prevent the data breach or to remedy it after it occurred. *Read more*

DATA PRIVACY

Virtual Private Network (VPN) Providers: How Private Are They?

By Executive Order (EO), the Trump Administration recently reversed an Obama Administration order aimed at protecting consumers' personal information from use by their Internet Service Provider (ISP). Prior to the Trump's EO, ISPs were required to get a customer's

consent before using or selling their browsing habits, online shopping habits, financial information, etc. The reversal of Obama's protection order has caused a resurgence of interest in VPN services. In theory, using a VPN service creates an encrypted tunnel between your device and the service provider, thus keeping your browsing habits and personal information private from your ISP. *Read more*

DRONES

How a Drone Could Save a Life at an Industrial Jobsite

According to the Occupational Safety and Health Administration (OSHA), 4,836 workers were killed on the job in 2015—that means, if you break it down, more than 90 workers lost their lives each week on jobsites. These jobsite deaths were more likely to occur in industries such as construction, inspection, and mining. In addition to this horrifying statistic, workplace injuries and illnesses cost U.S. employers approximately $1 billion per week in workers' compensation costs alone, with lost productivity, staffing replacements, and repairs to damaged equipment resulting in additional loss. Because of these staggering statistics, many companies are turning to drones to inspect jobsites and identify potential hazards before they become dangerous. *Read more*

Indiana Bill to Create New UAV-Related Misdemeanors

S.B. 299, introduced by Senator Eric Koch, has passed the Indiana General Assembly and is on its way to the desk of Governor Eric Holcomb for his final consideration. S.B. 299 would create Class A misdemeanor offenses specifically related to unmanned aerial vehicles (UAV or drones) to address the public's concerns on voyeurism, harassment, and public safety. Koch said, "While the development of drone technology has a substantial benefit for society, we need to ensure they are not used to commit crimes." *Read more*

The FAA's New Study on UAS Human Collision Hazards

The Federal Aviation Administration (FAA), along with a group of universities, conducted a study to determine the risks associated with flying unmanned aircraft systems (UAS) over people. Through the Alliance for System Safety of UAS through Research Excellence (ASSURE), the group of universities included the University of Alabama-Huntsville, Embry-Riddle Aeronautical University, Mississippi State University, and the University of Kansas. ASSURE's research began back on September 20, 2016. Upon completion of the studies, the FAA, personnel from the National Aeronautics and Space Administration (NASA), the U.S. Department of Defense (DoD), and other subject matter experts conducted a peer review of the

findings. *Read more*

FAA Releases Airport Facility Maps for Safer Drone Operations

As we discussed in our previous post, the Federal Aviation Administration (FAA) published over 200 airport facility maps last week to aid drone operators in safer operation and streamline the authorization process for commercial drone operations. The FAA plans to publish additional maps every 56 days through the end of 2017, which coincides with the FAA's preexisting 56-day aeronautical chart production schedule. *Read more*

PRIVACY TIP #86

Android Users Vulnerable to Malware through Apps

University of Michigan researchers have discovered that hundreds of applications in Google Play turn Android phones into a server that allows the user to connect the phone directly to a PC and leave open insecure ports available on the smartphone.

What does this mean? It means attackers can use the open insecure port to get into the smartphone and steal data, contacts, photos, and music, and install malware.

The researchers scanned 100,000 popular apps in the Google Play app store to determine if any of them allowed users to connect directly to their PC to send text messages, transfer files, or use the phone to connect to the Internet. They found 1,632 apps allowed the connections, and of those, 410 had no or weak protection in allowing access to open ports. 57 of those were completely open, basically allowing any hacker access.

Two apps are being called "particularly dangerous." Wifi File Transfer, which has more than 10 million downloads, allows an attacker to get full access to the phone because there is no authentication. The second, AirDroid, allows Android users full control of their PC through their Android phone. Because of an authentication flaw, malicious intruders could gain access through the port. When the researchers alerted the developers of the app, they patched it.

Nonetheless, numerous apps are available through Google Play that contain this flaw. It is important to note that neither Google nor the user can fix the flaw—it is up to the app developers. The only thing you can do is to uninstall the vulnerable app.

The tip this week is that, no matter what kind of smartphone you own, be cautious when downloading apps, including reading the app's Privacy Policy and Terms of Use and keeping up-to-date on vulnerabilities of apps that you have on your phone. Although they are

convenient, not all apps need to be downloaded.