Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

New IBM/Ponemon Study Shows Low Organizational Cyber Resilience

A new IBM/Ponemon Study released late last week, *2016 Cyber Resilient Organization*, reveals that only 32 percent of IT and security professionals believe that their organization has a "high" level of cyber resilience. The study interviewed 2,400 IT and security personnel across the world. *Read more*

NIST Releases Guidance on Internet of Things

The National Institute of Standards and Technology recently released guidance for the makers of devices that use or are connected to the Internet to build robust security measures into the design of products from the get-go. The Guidance—NIST Special Publication 800-160, is the culmination of four years of research, and focuses on the engineering functions that need to be addressed during the design of products connected to the Internet of Things (IoT). *Read more*

DRONES

FAA Sends Proposed Rule for Drone Flights Over People to the White House OIRA

Last week, the Federal Aviation Administration (FAA) proposed a new rule for performance-based standards and means-of-compliance for operation of small unmanned aircraft systems (UAS or "drones') over people who are not directly participating in the drone operation. This is contrary to the Small UAS Rule (or Part 107 as it is commonly called), which explicitly prohibits drone flights over people without a proper Part 107 waiver. *Read more*

ENFORCEMENT + LITIGATION

November 23, 2016

FEATURED AUTHORS:

Linn Foster Freedman
Sean Lawless
Kathryn M. Rattigan

FEATURED TOPICS:

Cybersecurity
Drones
Data Security
Enforcement + Litigation
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

FINRA Fines Lincoln Financial Group $650,000

A Lincoln Financial Group subsidiary has agreed to accept a $650,000 fine levied against it by the Financial Industry Regulatory Authority (FINRA) and to implement more robust security controls for a 2012 hacking that compromised the personal information of approximately 5,400 customers. This case is important and clear guidance to FINRA regulated entities. *Read more*

Facebook Calls Illinois Biometric Law Unconstitutional

In the ongoing saga of Facebook's challenge of the Illinois Biometric Law, it declared last week that the Illinois law violates the United States Constitution.

According to Facebook's Answer in a suit filed against it in California, the law is unconstitutional because it violates the Commerce Clause, which limits states from enacting legislation that would burden interstate commerce. In this case, Facebook is saying that not allowing it to use biometric analysis software to scan photographs posted by users in Illinois restricts its ability to use the data in commerce and therefore, its ability to engage in interstate commerce.

Facebook has also filed a Motion to Dismiss the entire case, which is pending. *Read more*

DATA SECURITY

International Cellular Roaming – Am I Secure?

Many firms have strict international travel policies in relation to the use of technology. These policies tend to be more skewed towards countries with greater state control over communications networks and specifically the Internet. However, the reality is that you are vulnerable whenever your device is roaming internationally. This is nothing particularly new or eye-opening for security experts. What is somewhat new is the Long-Term Evolution (LTE) standard. *Read more*

PRIVACY TIP #62

PoisonTap Can Compromise Computer with USB Stick

Security researcher Samy Kamkar has announced that a new hacking tool—PoisonTap—can be loaded onto a USB stick and used to hijack the Internet connection of one's computer.

The way it works is that if someone leaves their computer unattended, a hacker can stick the USB drive into the unattended laptop and although the individual may be accessing information through a VPN, PoisonTap takes over the Internet traffic, and continues to work even after the USB drive is removed.

According to Kamkar, when PoisonTap is introduced into a device, it masquerades as an Ethernet device and requests the IP address, even if it is locked or password protected. Then the computer sends all of its Internet traffic though PoisonTap. It will send any requests to the Web and steal cookies from over one million web sites, which can allow the attacker to automatically log into sites without a username or password. It can also redirect requests to the attacker's site, which gives the attacker control over browsing.

The tip in response to this new attack?

Do not ever leave your laptop unattended (like on the train or in any other public place like a coffee shop). As we have mentioned before, review and put in place procedures that limit employees' ability to introduce any foreign USB drives into the network, and provide employees educatin around the risks of USB drives, including PoisonTap.