Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

Chilean Bank Struck by "Virus" that Steals $10 Million

Just weeks after Mexico's central bank was targeted by hackers who stole $15 million, Chile's biggest bank, Banco de Chile, announced on May 28, 2018, that it had been struck by a "virus" that affected its workstations, including malware that contained disk-wiping capabilities. The malware sabotaged approximately 9,000 master boot records of the bank's computers and servers, which caused internal operations to practically cease.

It is reported that the ransomware was similar to NotPetya, crashed more than 500 servers and 9,000 of the bank's computers, and was able to wipe out disks and destroy forensic data.

This is the most recent of a series of attacks against banks, which affects online, branch and telephone banking. All the more reason to consider different banking options and to print your bank statements every month [related privacy tip]. *Read more*

Hackers Steal $31 million in Cryptocurrency from Bithumb

Bithumb, located in South Korea and ranked the seventh largest cryptocurrency exchange, has confirmed that it was hacked and that the thieves absconded with approximately $32 million in coins, including the XRP token issued by Ripple.

Following the hack, the exchange stopped processing cryptocurrency deposits and withdrawals and moved assets offline. Bithumb has reported that it will compensate victims for the losses. *Read more*

DATA PRIVACY

U.S. Supreme Court Issues Seminal Privacy Decision Concerning Cell Location Data

Cell phones are a ubiquitous part of our modern life. It's easy to forget

June 28, 2018

FEATURED AUTHORS:

Conor O. Duffy
Linn Foster Freedman
Jessica A.R. Hamilton
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

that they are constantly tapping into the wireless networks around us several times a minute, even when we're not using them. Each time a cell phone connects to a cell tower or cell site, it generates a time-stamped record known as Cell-Site Location Information (CSLI). Wireless carriers collect and store their customer's increasingly precise CSLI generated from incoming calls, text messages, and routine data connections. Would you expect these CSLI records maintained by your service provider to remain private? What if the police wanted access to them as part of an investigation of a crime? Should they be expected to obtain a warrant in order to obtain them? *Read more*

ENFORCEMENT + LITIGATION

Supreme Judicial Court Rules Robocalls are Harassment

This week the Massachusetts Supreme Judicial Court (SJC) ruled in favor of a consumer who sued Target alleging that it harassed her with robocalls.

The plaintiff applied for a Target credit card, and subsequently fell behind in payments. Starting in January 2015 Target contacted the debtor in an attempt to collect the debt. According to the consumer, Target called her up to six times a week, and Target admitted to calling her five times a week. Target argued that because it called the debtor with an automatic dialing service and did not leave a message, that it did not "initiate" a call with the debtor. *Read more*

Credit Reporting Agencies Now Must Register with NY DFS and Comply with Cybersecurity Regulations

The New York Department of Financial Services (DFS) issued new regulations requiring every consumer credit reporting agency that "assembles, evaluates, or maintains a consumer credit report on any consumers located in New York State register with the Superintendent of the Department of Financial Services." As a result of those agencies' new status of having to register with DFS, credit reporting agencies are subject to annual reporting and enforcement by DFS. *Read more*

DATA BREACH

Connecticut Expands Consumer Protections Against Identity Theft and Data Breaches

On June 4, 2018, Connecticut Governor Dannel P. Malloy signed into law Public Act No. 18-90 "An Act Concerning Security Freezes on

Credit Reports, Identity Theft Prevention Services and Regulations of Credit Rating Agencies" (PA 18-90). This bill makes several revisions to Connecticut laws concerning identity theft, most notably by newly prohibiting credit reporting agencies from charging fees for consumers to place or remove security freezes. This law takes effect on October 1, 2018. *Read more*

DRONES

Report Says Large Companies Using Drones See Positive ROI in Under a Year

Skyward, a provider of drone operations management software and consulting services, recently released the results of a Blue Research survey indicating that one in ten U.S. companies with revenue of more than $50 million are utilizing drones. Of those companies, 92 percent have realized a positive return on investment (ROI) in one year or less. Additionally, the report suggests that drone use among these companies could reach about 12 percent by the end of 2018. *Read more*

PRIVACY TIP #145

Print Your Bank Statements

How do you track your bank balances? This week's privacy tip focuses on the reasons consumers should print their bank statements, including several recently reported hacking and malware issues at banking institutions. *Read more*