Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

Governor Cuomo Unveils Cybersecurity Proposals Including Cyber Incident Response Team

New York Governor Andrew Cuomo announced a series of cybersecurity proposals that are designed to protect consumers and government entities from cybercrime and identity theft. One of the proposals includes the creation of a Cyber Incident Response Team that would support state and local government bodies, critical infrastructure, and schools. It will be led by the state Division of Homeland Security and Emergency Services within the Counter Terrorism Unit. *Read more*

Studies Show Ransomware Up 6,000 percent and Reaps Billions and Phishing Emails Are Used in 91 percent of all Cyber-Attacks

A recent IBM study shows that ransomware increased 6,000 percent in 2016 over 2015. According to the report, ransomware was present in almost 40 percent of all spam email messages. A recent PhishMe study also found that over 91 percent of cyber-attacks start with spear phishing emails. *Read more*

No More Ransom Project Expands Membership and Tools

The No More Ransom Project, a coalition of security companies and law enforcement, that was launched through a partnership with the European Cybercrime Centre, the National High Tech Crime Unit of the Netherlands police, Kaspersky Lab, and Intel Security, has added 30 new members and 32 new decryption tools to combat ransomware variants. *Read more*

DATA BREACH

U.S. Military Special Operations Command Workers' Data Exposed by Vendor

Military personnel continue to be victimized by data breaches. This time, the personal information of health care workers employed by

January 12, 2017

FEATURED AUTHORS:

Linn Foster Freedman
Carly Leinheiser
Kathryn M. Rattigan
Jean E. Tomasco

FEATURED TOPICS:

Cybersecurity
Enforcement + Litigation
Data Breach
Data Privacy
Drones
HIPAA
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

Potomac Healthcare Solutions (Potomac), who work for a U.S. Special Operations Command, were exposed. The Potomac health care workers travel to provide Navy SEALs, Army Green Berets and Rangers, Delta Force members and the Air Force, and Marine commandos with health care services. *Read more*

New Hampshire Psychiatric Hospital's Patient Records Posted Online by Former Patient

The New Hampshire Department of Health and Human Services has notified up to 15,000 patients of its psychiatric hospital (New Hampshire Hospital) that their names, addresses, Social Security numbers, Medicaid ID numbers, and highly sensitive psychiatric health information was posted on a social media site by a former patient. *Read more*

HIPAA

Three-Month Delay Means Health Network Must Pay

A delay in reporting a HIPAA violation can result in a significant monetary penalty. That was the message sent by the Office for Civil Rights (OCR), which recently announced the first HIPAA settlement based on the untimely reporting of a breach of unsecured protected health information (PHI). According to the OCR, Presence Health (a large health care network in Illinois) has agreed to settle potential violations of the HIPAA Breach Notification Rule by paying $475,000 and implementing a corrective action plan. *Read more*

Pagers Compromised, Exposing Health Information of Patients

Providence Health & Services, a health system located in Alaska, California, Oregon, Montana, and Washington, has reported that its paging system has been breached. An unauthorized individual was able to intercept pages between health care workers and post the contents online between October 25 and October 28, 2016. *Read more*

ENFORCEMENT + LITIGATION

FTC Charges Taipei-Based D-Link for Inadequate Security of Computer Routers and Cameras

The Federal Trade Commission (FTC) has filed a complaint in Northern California against D-Link for putting thousands of consumers at risk over the past decade for failing to have adequate security practices in its routers and cameras. *Read more*

DATA PRIVACY

501(c)(3) Public Charities Subject to New Donor Disclosure Requirements in New York

Since 1958, when the Supreme Court held that the State of Alabama's attempt to compel the NAACP to disclose its membership lists infringed on the members' constitutional rights to freedom of speech and assembly, charities and donors have expected donor information to remain confidential. However, recent developments in New York have thrown that expectation into question. *Read more*

DRONES

FAA Updates the Public on Drones with "A Story of Revolution and Evolution"

At the CES Unmanned Systems conference in Las Vegas last week, Federal Aviation Administration (FAA) Administrator Michael Huerta provided the public with an update on the state of our unmanned aircraft systems (UAS) in the United States and how the FAA plans to grow the UAS industry in the coming year. *Read more*

Update on the Drone Flights-Over-People Rule

The Federal Aviation Administration (FAA) continues to work on its proposed rule, which would allow the operation of unmanned aircraft systems (UAS) over people, expected (hopefully) to be released before the end of the Obama Administration next week. For the final rule, of course, there is no set timeline. FAA Administrator Michael Huerta did say, however, "I can give you my steadfast commitment that we are doing all that we can to advance this effort. And we will be looking to our industry partners to work with us to develop more ingenious ways to ensure that drones are able to fly over people without sacrificing safety or security." As we noted in our previous post, this rule would greatly expand UAS operations across many different industries. *Read more*

PRIVACY TIP #69

Hit with Ransomware? To Pay or Not to Pay

Every day I get a call from a client asking for help involving ransomware. Friends have called in a panic when that dreadful message comes up on the screen informing you that you are the

victim of ransomware with instructions on how to pay the ransom with bitcoin. It is no longer a surprise to get those calls. They are a mundane and sad part of the life of a privacy and security lawyer.

I love to read mysteries, whodunits filled with murders and kidnappings. Real stories of kidnappings in movies and books back in the day were based on the premise that, if you paid the ransom, the perppetrators would come back for more. If you paid the ransom, the crime would never cease. And if you paid it, you were never sure that you would get your loved one back. Remember when law enforcement was always on the other line during the phone call, coaching the family on how to negotiate with the kidnapper? Refusing to pay the ransom and setting up a trick for the drop of the money always worked and justice prevailed!

Now I am not equating the kidnapping of a loved one with computer ransomware, but admittedly, there are similarities. When did data get so important that we have abandoned as a nation the notion of refusing to pay the kidnapper?

Law enforcement continues to recommend that companies refuse to pay ransom for data. Companies continue to not be fully prepared for a ransomware attack with robust data back-up, incident response, contingent operations, and business interruption, so they are paying the ransom. The IBM study showed up to 70 percent of businesses are paying the kidnappers!

Folks, no wonder our data continues to be kidnapped. It is a great way for criminals to make money, and if we keep paying the kidnappers, the more they will kidnap.

In 2017, let's collectively work together to stop the kidnappers by refusing to pay them for our beloved data. That means we must all be prepared for a ransomware attack, combat it, and give the kidnappers incentive to go elsewhere.