



Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks



CYBERSECURITY

[New York's Landmark Cybersecurity Regulation Compliance Deadlines Looming](#)

On February 15, 2018—that is, today—banks, insurance companies, and other financial services institutions and licensees regulated by the New York Department of Financial Services (DFS) are required to file their first certification of compliance with DFS' far reaching cybersecurity regulation (23 NYCRR Part 500) (the "Regulation").

The Regulation, which became effective on March 1, 2017, is touted as being the first cybersecurity regulation in the nation, requiring significant operational, technology, and reporting changes in order for entities covered by the Regulation (Covered Entities) to comply. [Read more](#)

ENFORCEMENT + LITIGATION

[Ciox Health, LLC Initiates Lawsuit against the Department of Health and Human Services Over Medical Records Request Fees under HIPAA and HITECH](#)

On January 8, 2018, Ciox Health, LLC (Ciox) filed a [complaint](#) against the Department of Health and Human Services (HHS) and then-acting Secretary Eric D. Hargan, alleging that the Department's rules and guidance under HIPAA and HITECH, "impose tremendous financial and regulatory burdens on health care providers and threaten to upend the medical-records industry that services them." The complaint claims that the Department's 2013 omnibus rule and 2016 guidance violated the Administrative Procedures Act, and it asks District Judge Amit Mehta of the United States District Court for the District of Columbia to declare those acts unlawful and further enjoin HHS from further enforcing either of them. [Read more](#)

HIPAA

[OCR Warns of Cyber Extortion and Provides Checklist](#)

In its January [newsletter](#), the Office for Civil Rights (OCR) focused on cyber extortion, which it stated has "risen steadily over the past couple of years and continues to be a major source of disruption for many organizations." Since the health care industry has been the target of cyber extortion attacks, the OCR is specifically warning health care entities and has published a checklist to help HIPAA covered entities and business associates respond to a cyber-

February 15, 2018

FEATURED AUTHORS:

[William M. Daley](#)
[Linn Foster Freedman](#)
[Benjamin C. Jensen](#)
[Kathryn M. Rattigan](#)
[Norman H. Roos](#)
[Scott N. Siedor](#)
[Carrie C. Turner](#)

FEATURED TOPICS:

[Cybersecurity](#)
[Drones](#)
[Enforcement + Litigation](#)
[HIPAA](#)
[Privacy Tip](#)
[Virtual Currency](#)

VISIT + SHARE:

[Insider Blog](#)
[R+C website](#)
[Twitter](#)
[Facebook](#)
[LinkedIn](#)

attack. [Read more](#)

VIRTUAL CURRENCY

Nationwide, State Legislators Push Blockchain-friendly Legislation

As previously reported, state legislatures throughout the country continue to propose legislation designed to facilitate the use of blockchain-based technology by businesses within their states. In recent weeks, legislatures in Florida and Nebraska have each proposed laws streamlining the transaction of business electronically and through use of distributed ledgers on blockchain applications. In Arizona, the state senate just passed a bill allowing residents to pay income taxes through a cryptocurrency such as Bitcoin. [Read more](#)

DRONES

World-Record Drone Show at Olympic Ceremony

As with any Olympics Opening Ceremony, the pageantry is of global scale, but this year, in Pyeongchang, South Korea, Intel took it to a whole new level –a record-setting 1,218 drones hit the skies for a mechanical phenomenon. There's never been anything like it.

Intel's Shooting Star software platform enables an army of one foot-long, eight ounce, plastic, and foam quadcopters to fly in sync along an animator's pre-determined path. General Manager of Intel's drone group, Anil Nanduri, said, "It's in essence technology meeting art." [Read more](#)

DJI Software Now Includes Temporary No-Fly Zone for Olympics

Drone manufacturer, DJI, has updated its software in its drones to include a temporary no-fly zone around the Olympic Games in Pyeongchang, South Korea (and other South Korean cities). The parameters of the no-fly zone are based on four zones in Pyeongchang, Gangneung, Bongpyeong, and Jeongseon in Gangwon Province. DJI made this decision to implement this no-fly zone in an effort to increase safety and security measures. The no-fly zone will be removed at the conclusion of the games later this month. [Read more](#)

More Passenger Drone Test Flights Hitting the Skies

We previously reported on the [Y6S drone passenger test flights](#) set for this year in London; now, two more companies have started testing passenger drones. Ehang 184 passenger drones, created by the Chinese company Beijing Yi-Hang Creation Science & Technology Co., Ltd., and Vahana, Airbus' passenger drone project, both hit the skies. [Read more](#)

PRIVACY TIP #126

Employee Training and Education Continues to be “Best” Cyberdefense

It is a myth that employees hate training and education. I have seen it with my own eyes. It is very exciting to watch an audience visibly cover their mouths when real life stories are told about cyber-attacks and phishing incidents that employees' conduct cause because they are working too fast, not paying attention to detail, and just plain don't know much about the risks of technology.

I am constantly amazed the number of people of all ages who have no idea about the risks posed by the use of technology, and how they can put themselves and their companies at risk by one click.

Arming employees with tools to protect your digital perimeter gives them a sense of purpose and pride. In my experience, employees do not want to be the one who clicks on the link that introduces malware or ransomware into the company system. I have never seen a victim who has enabled an infiltrator into the system feel anything except horror. Employees in general really do want to do a good job for their company and do not want to harm it.

That's why employee training and education in data privacy and cybersecurity continues to be so important as a mitigating factor to the risk of cyber intrusions. According to a survey of cybersecurity professionals in financial firms, in their opinion, employee education and training on data privacy and security is the best defense against cyber-attacks—over network security breach prevention, or securing the cloud. This is because “[P]rotective measures on a firm's computer system can still fail if a worker click on a link or downloads an email attachment carrying malicious code.” So true.

Most employees don't understand the risks until you show them and tell them real stories that they can relate to, learn from, and not replicate. Face to face training works wonders for increasing the culture around data privacy and security and empowers employees to assist companies in promoting practices to protect data. Try it—you will be surprised at how engaged your employees can be when they are part of fixing the problem.

Boston | Hartford | New York | Providence | Stamford | Albany | Los Angeles | Miami | New London | rc.com

Robinson & Cole LLP

