Attorney Advertising

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

Think Tank Says Nuclear Missiles Can be Inadvertently Launched Through Cyber-Attacks

Just before the false alarm in Hawaii last weekend when residents were erroneously warned of an impending missile attack, think tank Chatham House issued a report stating it had identified vulnerabilities in nuclear weapons systems worldwide that made them susceptible to malware and ransomware attacks that could lead to inadvertent missile launches.

This is a scary report. It notes that the computer systems which control nuclear weapons systems were developed when computers were in their infancy and malicious cyber activities were not contemplated or experienced. Because data security was not built into the architecture of the nuclear control systems, the systems could be tampered with unbeknownst to its controllers. *Read more*

ENFORCEMENT + LITIGATION

Connecticut Supreme Court Recognizes Common-Law Cause of Action for Unauthorized Disclosure of Confidential Medical Information

In a long-awaited decision concerning the confidentiality of medical records and patient privacy, the Connecticut Supreme Court recently concluded that the physician-patient relationship establishes a duty of confidentiality to a patient in Connecticut, and unauthorized disclosure of confidential information obtained for the purpose of treatment in the course of that relationship gives rise to a cause of action in tort, unless the disclosure is otherwise permitted by law. In *Byrne v. Avery Center for Obstetrics and Gynecology, P.C.,* the Court considered—for a second time—the legal implications arising from the defendant's mailing of the plaintiff's medical records in 2005 to a probate court in response to a subpoena without providing notice to the plaintiff, filing a motion to quash the subpoena, or appearing in court as requested under the subpoena. *Read more*

January 18, 2018

FEATURED AUTHORS:

Scott M. Baird
Nuala E. Droney
Linn Foster Freedman
Kathryn M. Rattigan
Norman H. Roos

FEATURED TOPICS:

Cybersecurity
Data Breach
Drones
Enforcement + Litigation
Privacy Tip
Virtual Currency

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

DOJ: Seek Data from the Business Enterprise, Not Its Cloud Provider

Where does the U.S. Department of Justice (DOJ) turn when it needs business enterprise data stored on the cloud for a criminal investigation? According to a recent DOJ memo, the default rule is now to turn to the business enterprise first and the cloud only if necessary: “prosecutors should seek data directly from the enterprise, if practical, and if doing so will not compromise the investigation.”

The DOJ addressed the issues that arise when enterprises (“companies, academic institutions, non-profit organizations, [and] government organizations”), pay cloud providers to store data. Before the cloud, prosecutors would have to obtain the data from the enterprise’s own servers. Now with outsourced cloud storage, prosecutors could technically side-step the enterprise and obtain that data from the cloud providers. *Read more*

VIRTUAL CURRENCY

Another Hitch in the Crypto Boom? North Korean Malware Hijacks Computers to Mine Monero Cryptocurrency

Researchers at cybersecurity firm AlienVault have discovered a computer virus of North Korean origin which infects and hijacks computers in order to mine Monero, a private digital currency which styles itself as “secure, private and untraceable.” Cryptocurrency mining is the resource-intensive process by which computers or “miners” running specific software verify cryptocurrency transactions. In exchange for their computing power, miners are given small amounts of cryptocurrency. In the case of North Korean’s Monero malware, the virus installs mining software on infected computers unbeknownst to their owners or users. The software then secretly mines Monero and sends mining rewards back to a server located at Kim Il Sung University in Pyongyang. Researchers are unsure how many computers may be affected. *Read more*

DATA BREACH

Hancock Health Hit with Ransomware That Shuts Down Network

It has been predicted that the health care industry will continue to be lambasted with ransomware in 2018. It has also been predicted that attackers will move from taking sensitive information hostage to sabotage, service disruption, physical damage, and malicious deletion or changes to the integrity of data. Unfortunately, the year has started off true to the predictions. Last week, Hancock Health, located in Indiana, was hit with a ransomware attack that it describes as

"sophisticated," and it did not occur as a result of an employee opening an infected email. *Read more*

DRONES

U.S. Drone Registration Celebrates the 1 Million Mark

The Federal Aviation Administration (FAA) recently announced that the total number of drones now registered has surpassed one million. That one million registration figure includes 878,000 drone hobbyists, who receive only one registration number for all the drones they own—which means they likely own more than one, and that 878,000 number means there are even more drones in the sky than that. The other 122,000 drone registrations include commercial, public, and 'other' drones which are all individually registered with the FAA. It is also important to note that these drone registrations are for all drones [or unmanned aircraft systems (UAS)—the official name of these flying devices] weighing over 0.55 pounds but under 55 pounds in total (i.e., including payloads, onboard cameras, etc.). This one million registration number is even more astounding because so many hobbyist drones weigh less than 0.55 pounds, and there are certainly other types of commercial drones weighing over 55 pounds that are zipping around the skies. *Read more*

New York Governor Announces Drone Fleet for its State Police

Last week, Governor of New York Andrew Cuomo announced the launch of a new State Police Unmanned Aerial System (UAS) program, which will be used for law enforcement missions, including, but not limited to, disaster response, traffic safety, and crime scene investigation. To start, the program will launch four state police drones –Troop A, which will serve eight counties in western New York; Troop D, which will serve seven counties in central New York; Troop F, which serves five southern counties west of the Hudson River; and Troop G, which serves 10 counties in the Capital Region. An additional 14 drones will be launched by April 2018. Governor Cuomo said, "This state-of-the-art technology will improve emergency response, improve operational and cost efficiency, and increase troop safety." *Read more*

Rail Inspection Firm Acquires Drone Services Company

American Rail Engineers Corp. (ARE), based in Irvine, California, recently acquired a New Hampshire drone services company, Media Wing, LLC (Media Wing), to conduct geographic information system (GIS) mapping and data analytics and enhance ARE's remote sensing and data processing capabilities. ARE is a bridge

management and safety services business for private railroads and public transportation authorities. ARE hopes to expand its engineering and software development by using Media Wing's advanced data collection and video production skills and tools. These two companies together will allow ARE to add value to the deliverables it provides to its clients by allowing for more data collection, better image analysis, GIS modeling, and video-rendering. This is yet another example of how drones are finding their way into all types of industry and now, more than ever, our nation's infrastructure. *Read more*

PRIVACY TIP #122

What's Up with WhatsApp's Security Flaws?

WhatsApp has been applauded for adding end-to-end encryption on its platform to secure conversations of its users two years ago. But encryption has its challenges, despite its security posture.

Recently, a team of German cryptographers found flaws in WhatsApp that they say makes it easier for unauthorized individuals to access group chats. They also found flaws with Signal and Threema, which have been reported to be harmless.

What the researchers claim is that an administrator of a conversation can invite new people into a conversation. But when the administrator invites those new people, the WhatsApp server doesn't authenticate the new member, and therefore, anyone controlling the server could insert new people into the private conversation without the administrator's knowledge. According to the researchers, the servers themselves should not be able to read the messages or insert new people into the conversation without the knowledge of the administrator, but this is what can happen.

If a new member to the group is added through the server, that member has access to secret keys from every other participant in the group, which gives the intruder full access to all future messages. Some people use WhatsApp for highly sensitive conversations, which they don't want unauthorized individuals to have access to.

The takeaway is that administrators and users in WhatsApp groups should watch carefully when new members are invited and join, and warn other members of an interloper or a spoofed invitation message. The administrator of the group can remove the unauthorized member and inform the legitimate users in a one-to-one message of the intruder, and can start a new group and invite only intended members.