Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

Medical Device Malware Medjack.3 Poses Threat to Hospitals

Medjack is a form of malware that was specifically developed to attack medical devices, such as heart monitors, CT and MRI machines, insulin pumps, and PAC systems. Medjack has been in existence since 2015, and Medjack.2 came on the scene in the summer of 2016. Medjack.2 was able to bypass security controls and use cybersecurity tools to install backdoors and move within a health care system without notice. Security researchers at TrapX have now discovered a third version of Medjack, dubbed Medjack.3, where hackers are using an old malware spreader to attack medical devices connected to older operating systems. *Read more*

ENFORCEMENT + LITIGATION

Yahoo Breaches Cost Shareholders $350 Million from Lowered Purchase Price, CEO Forfeits $14 Million in Compensation

Yahoo's troubles for failing to timely disclose security breaches provides rare insight into quantifying the financial and other costs to a company's shareholders and leadership when a security breach occurs and is mishandled. This week, it was also disclosed that senior executives managing Yahoo at the time of the breaches would face consequences. Yahoo's legal counsel was forced out. CEO Marissa Mayer said she voluntarily gave up her 2016 annual cash bonus and 2017 stock award, which together are worth about $14 million. *Read more*

DATA BREACH

West Virginia University Medicine's University Healthcare Patients Victims of Identity Theft

West Virginia University Medicine's University Healthcare (WVUM) has confirmed it is sending notification letters to over 7,400 of its patients seen at Berkeley Medical Center as a result of an unauthorized access to their information. It further confirmed that 113

March 9, 2017

FEATURED AUTHORS:

Kate E. Dion
Conor O. Duffy
Linn Foster Freedman
Benjamin C. Jensen
Kathy M. Porter
Kathryn M. Rattigan

FEATURED TOPICS:

Cybersecurity
Enforcement + Litigation
Data Breach
Data Privacy
Health Information Privacy
Drones
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

of its patients have become the victims of identity theft as a result of the theft of patient records by an employee of Berkeley Medical Center. *Read more*

Data Breach Involving CloudPets "Smart" Toys Raises Internet of Things Security Concerns

On February 27, 2017, news reports disclosed a major security breach involving Spiral Toys, the seller of the CloudPets brand of internet-connected stuffed animals. The Bluetooth-connected CloudPets toys allow users to exchange voice messages between the toys and applications on smartphones or tablets. An investigation by cybersecurity researcher Troy Hunt revealed that customer data for over 800,000 registered accounts, including over two million voice recordings, was stored in an unprotected database on the public Internet. While the company has denied that any voice recordings were stolen, reports indicate hackers accessed the open database and attempted to ransom the data. *Read more*

Verifone Investigating Breach of its Internal Corporate Network

Verifone, the largest maker of credit card point-of-sale terminals in the U.S., which assists various industries, including retailers, with credit and debit card swipe and process services, has affirmed that it is investigating a breach of its internal corporate network. *Read more*

DATA PRIVACY

DOE and DOJ Withdrawal of "Dear Colleague" Letter Leaves FERPA's Guidance Unresolved

On February 22, 2017, the Department of Justice (DOJ) and the Department of Education (DOE) withdrew their May 13, 2016, "Dear Colleague" letter that provided guidance on steps to protect transgender students under Title IX of the Educational Amendments of 1972 (Title IX) as well as the Family Educational Rights and Privacy Act (FERPA). Although the letter did not add any requirements to the law, it did provide guidance to covered entities as to how agencies would interpret and enforce the law. The decision by DOJ and DOE to withdraw the letter has clouded the issue and left its application to transgender students in question. *Read more*

HEALTH INFORMATION PRIVACY

Florida Supreme Court Rejects PSQIA Preemption of Florida

Constitution

On January 31, 2017, the Florida Supreme Court held that adverse medical incident reports produced in accordance with Florida law cannot constitute confidential and privileged patient safety work product (PSWP) under the federal Patient Safety & Quality Improvement Act of 2005 (PSQIA). In *Jean Charles, Jr. et al. v. Southern Baptist Hospital of Florida, Inc.* (No. SC15-2180), the Court endorsed a broad right of access under the Florida Constitution for patients to obtain adverse medical incident reports from health care facilities, a right commonly exercised by plaintiffs in medical malpractice actions. *Read more*

DRONES

An Update on Part 107 Waivers for Night Operations

Back in August 2016, when the Federal Aviation Administration (FAA) announced its final small unmanned aerial systems (UAS) rule (or Part 107), FAA administrator Michael Huerta said, "Our focus is to make this as streamlined as possible [. . .] We do not envision this being a very burdensome process." However, Part 107 limits flights that take place at night, beyond the visual line of sight, and above people—some of the most commonly sought-after operations for drones. But, since August, the FAA has issued over 300 Part 107 Waivers for just those types of operations. *Read more*

PRIVACY TIP #77

FTC Offers Tips to Businesses That Have Been Impersonated by Phishing Schemes

On March 6, 2017, the Federal Trade Commission (FTC) released tips and a video to businesses that have been impersonated by Phishing schemes.

The guidance, entitled "Has a phishing scam hooked your company's good name?" provides businesses with several tips to respond to being impersonated through a phishing scheme.

The tips include:

- Notify and alert customers through social media, email, and letters that you are being impersonated.
- Contact law enforcement.
- Provide resources to affected customers, such as referring them to www.identitytheft.com and the FTC's website.
- Review security practices and improve on any weaknesses

and lessons learned.

Although consumers are frequently the ones who we concentrate on when discussing phishing incidents, it is easy to forget businesses can be victims too. This guidance reminds us that businesses are being impersonated every day, and their brands are being harmed. Being prepared for this scam and responding appropriately are key to reducing harm to consumers and businesses.