Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

September 8, 2016

CYBERSECURITY

Dropbox Hacking from 2012 Actually Affected 68 Million Users

It was well known in 2012 that Dropbox suffered a data breach when its user names and passwords were compromised. But at the time, Dropbox did not admit the breadth of the compromise. Last week, Dropbox admitted that 68 million users' credentials were actually compromised in the 2012 hacking.

Apparently, Dropbox became aware of the full extent of the compromise when the online publication *Motherboard* obtained the database and the compromised files were available online.

So, basically, if Dropbox users have not changed their passwords since 2012, the files in Dropbox could be accessible by unauthorized individuals. Many companies use Dropbox for sensitive company information, deals, M&As, and intellectual property, much of which are the companies's jewels. If this information has been shared using the Dropbox application, it should be assumed it has been compromised.

Companies and individuals may wish to reconsider using Dropbox for their data, especially sensitive data, and all users should change their passwords immediately.

— Linn Foster Freedman

---

iPhones Vulnerable to Pegasus—Update Your iPhone Now

Apple has issued an urgent warning to iPhone users about a crucial iOS update that is the only way to protect iPhones from "the extremely malicious Pegasus software."

According to Apple, Pegasus can completely take over an iPhone, and only 86 percent of iPhone users have updated their phones by installing the iOS version 9.3.5.

Apple is urging all users to update their phones to eliminate the vulnerability. Employers who allow employees to use their iPhones for work purposes may wish to encourage their employees to update their iPhones to protect company data from Pegasus.

I updated my phone when the alert on my phone requested the update. Instead of clicking "later," update your phone now. It only takes a few minutes and is "crucial" according to Apple.

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

Connecticut State Police Lead the Way in Training Electronic Storage Device Dogs

The Connecticut State Police have taken the lead in training police dogs to be skilled in the art of detecting hidden data. As more and more crimes involve electronic evidence, criminal enforcement agencies throughout the country are recognizing the need to find that evidence quickly. Data-detecting dogs help do this by sniffing out chemicals associated with DVDs, USB drives, hard drives, SD cards, and micro SD cards. The Connecticut State Police started the program in 2012, specially training the first class of three dogs to detect evidence in computers and cell phones. The training is the work of not only the State Police K9 Unit but also the Connecticut Forensic Lab, where a chemist isolated a chemical compound used to coat memory boards in phones in computers and another chemical compound that exists in DVDs and CDs. The K9 unit then trained the dogs to recognize the smell of these compounds. In 2016, the K9 Unit graduated its second class of Electronic Storage Device (ESD) dogs, all labrador retrievers from Guiding Eyes for the Blind. The ESD dogs are now in the field sniffing out data for law enforcement agencies in Alaska, Missouri, Virginia, and Massachusetts as well for the FBI.

— Nuala E. Droney

DATA BREACH

Lightspeed Urges Customers to Change Passwords Following Data Breach

Lightspeed, a retail point-of-sale company that provides cloud-based services to 38,000 clients, has reported that its central database, which stores client information on sales, products, encrypted passwords, and in some instances, electronic signatures, has been compromised.

The system that was compromised was the one that retailers can access through tablets, smartphones, and, other mobile devices.

Lightspeed is suggesting that clients change their passwords. The compromise of the digital signatures is also concerning, so companies that receive the email notifying them to change passwords may wish to look further into the compromise of the digital signatures as well.

— Linn Foster Freedman

Information From 700-Plus Patients Stolen from LAC+USC Medical Center

Los Angeles County-USC Medical Center (LAC+USC) has notified patients that the protected health information of over 700 patients seen in the LAC+USC neurosurgery clinic was stolen from an employee's car. The information, which was contained on appointment lists, included patients' names, dates of birth, medical record numbers, telephone numbers, gender, and date/time of scheduled appointments and may also have included the reason for the examination and/or a patient's diagnosis.

With more and more health information being stored electronically, it is easy to forget that the privacy and security of paper records must also be protected. Tips for protecting paper records include storing them in a secure location (such as a locked file cabinet or portable document box), not leaving them unattended (such as in an automobile,) and shredding paper records when ready for disposal.

— Pamela H. Del Negro

MedStar Cardiology Employee Emails Patient Information to Personal Account and Gets Fired

MedStar Health Cardiology Associates (MedStar Cardiology,) affiliated with MedStar Health, which was recently in the news for a ransomware attack, discovered that an employee sent the protected health information of 907 patients to a personal email account.

The information contained in the email included the patients' names, dates of birth, health insurance ID numbers, and some Social Security numbers.

The affected patients were notified of the breach by mail on August 5, 2016, and are being offered identity theft protection. The employee was fired, and MedStar Cardiology is reeducating its employees on confidentiality of patient information.

This is a valuable lesson for health-care entities to educate employees about policies and procedures that prohibit the transfer of patient information to a personal email account.

— Linn Foster Freedman

PRIVACY TIP #51

Check Up on Your Tax Preparer's Data Security Measures

We have written before about the ability of hackers to file false tax returns to get fraudulent refunds by using the IRS website and how hundreds of thousands of Americans have become victims of tax fraud.

The IRS issued a statement last week warning tax preparers to be on the alert for hackings that allow criminals to hack into the tax preparer's system by using remote technology and then use the tax preparer's credentials to file a false tax return on behalf of his/her clients. The IRS indicated that it was aware of more than two dozen incidents in the past several weeks when false tax returns were filed through tax preparers' hacked systems.

The IRS warning came right on the heels of the Treasury Inspector General for Tax Administration's audit report of the IRS, which showed that almost 1.1 million taxpayers were victims of employment-related identity theft between February 2011 and December 2015.

The Inspector General's Report further found that 621,000 taxpayers were actually affected by tax fraud and that 355,000 taxpayers' accounts were actually breached by unauthorized individuals.

Your tax preparers have all of your most valuable personal information, that can be used to commit fraud if it gets into the wrong hands. Many tax preparers are solo or small companies, which may not have the

most sophisticated data security measures yet they have very valuable data.

Whether you to file taxes on a quarterly or yearly basis, it is a good idea to check with your tax preparer now (before the busy season), particularly with the IRS warning, to make sure s/he has "all available security measures on their tax preparation software." Send this blog post to your tax preparer to confirm that a robust security program is in place to protect your personal information, including security measures to prevent the system from being taken over remotely.

— Linn Foster Freedman

UPCOMING EVENTS

Authors' Events

In addition to their legal practice and involvement with the blog, our Data Privacy + Security Team members regularly serve as presenters at topic-related seminars and participate on panels that discuss developments in the relevant areas. The following are several upcoming speaking engagements:

- September 12 - 15 – (ISC)² Security Congress in Orlando, FL (Linn F. Freedman)
- October 11 & 12 – InfoGovCon in Providence, RI (Linn F. Freedman)
- October 24 - 26 – Privacy + Security Forum in Washington, D.C. (Linn F. Freedman)
- November 15 – ABA Webinar: "Assessing the Situation: How to Identify and Evaluate the Cyber and Data Risks that a Contractor Bears" (Linn F. Freedman)

For more thoughtful and timely discussions of legal news and perspectives on issues relating to data privacy and security, subscribe to our *Data Privacy + Security Insider* blog by e-mail or by RSS feed.

We welcome your feedback and ideas on topics you'd like us to cover. We also encourage you to share this *Insider* and the blog with anyone you think would find it useful.

If you have any questions, please reach out to your contact at Robinson+Cole or Linn F. Freedman, chair of our Data Privacy + Security Team.