Attorney Advertising

Robinson+Cole

Data Privacy and Security Insider

May 7, 2015

Data Privacy and Security Insider

DATA BREACH

Partners HealthCare Hit with Phishing Expedition Exposing 3,300 Patient Records

Late last week, Partners HealthCare announced that it notified approximately 3,300 patients of a security breach involving a hacking incident where intruders accessed medical and personal information of patients.

Partners acknowledged that the hackers were able to infiltrate the security of its system through phishing e-mails that employees opened, exposing their e-mail accounts to unauthorized intruders.

The information included in the exposed data included patients' Social Security numbers, addresses, telephone numbers and medical and health insurance information.

It is well-known that hackers are and will continue to target health care organizations and this is a strong reminder to health care entities to implement a strong employee training program to educate employees about e-mail phishing and other ploys commonly used by cyber criminals.

– Linn Foster Freedman

Verizon 2015 Data Breach Investigations Report Out

If you have never taken a close look at Verizon's yearly Data Breach Investigations Report, we highly recommend that you do. It just came out, and is once again, a very informative read.

The Verizon Report received data breach incident information from 70 contributing organizations in 61 countries, which reported on 79,790 security incidents, representing 2,122 confirmed data breaches.

The Report confirms that the top three industries affected are the "same as previous years: Public, Information, and Financial Services." But the conclusion is clear: "No industry is immune to security failures."

The grim news is that attackers are able to compromise an organization "within minutes" 60% of the time. For the past two years, "more than two-thirds of incidents that comprise the Cyber-Espionage pattern have featured phishing." (See Partners HealthCare breach post above). Almost 50% of individuals "open e-mails and click on phishing links within the first hour" of receiving them. The Report reiterates how important education and training is for your employees to detect and mitigate phishing expeditions.

Interestingly, the Report indicates that mobile devices are "not a preferred vector in data breaches." Remember though, that this Report focuses on infiltration, not loss, so don't take your eye off the mobile

device ball.

The authors provide a new model for forecasting the cost of a data breach which is quite helpful. Take a look at the numbers on page 30 of the Report. They state that the numbers are given with a 95% confidence rate in the expected column, which shows the cost for 100 records at $25,450; 1,000 records at $67,480; 10,000 records at $178,960; 100,000 records at $474,600; 1,000,000 records at $1,258,670; 10,000,000 at $4,448,020; and 100,000,000 (e.g. Anthem) at $8,852,540.

Finally, the Report follows the 2014 Report by classifying incidents into 9 categories. This year the Report concludes that incidents are caused 29.4% from miscellaneous errors; 25.1% by crimeware; 20.6% from insider misuse; 15.3% from physical theft/loss; 4.1% from web app attacks; 3.9% from denial of service; 0.8% from cyber-espionage; 0.7% from POS intrusions; and 0.1% from payment card skimmers.

Hats off to the guys at Verizon for their superb work every year on this Report. It is chock full of useful information and is a must read for privacy and security professionals. Show them your support by reaching out to them at dbir@verizon.com. I just did.

– Linn Foster Freedman

HEALTH INFORMATION

Hospital CFO Must Pay $4.4 Million For Falsely Attesting To Meaningful Use

The Health Information Technology for Economic and Clinical Health Act, adopted in 2009, pumped billions of dollars into hospitals and physicians (through the Centers for Medicare and Medicaid) in order to stimulate them to adopt electronic health records. To receive the economic incentives, hospitals and physicians had to "attest" to using electronic health records in a meaningful way over the past several years. This was no easy task, and the criteria and reporting obligations were and continue to be significant for health care providers.

Last November, the CFO of Shelby Regional Medical Center in Texas pled guilty to falsely attesting to the meaningful use program on behalf of the hospital during the 2012 reporting period. He also pled guilty to aggravated identity theft for using a hospital worker's name to falsely attest to meaningful use.

The false attestations resulted in Shelby and other hospitals owned by Tariq Mahmood to receive close to $17 million in incentive payments from CMS. Mahmood was sentenced to 11 years in prison for the health care fraud last month.

The CFO has agreed to pay $4.4 million in restitution for his part in the fraudulent scheme. He will be sentenced later this month and could get up to seven years in federal prison.

CMS has been actively auditing both hospitals and physicians who have attested to meaningful use, and this case underscores CMS' seriousness of rooting out health care fraud.

– Linn Foster Freedman

JAMA Releases Study Analyzing Scope and Characteristics of Recent Data Breaches

Reports of security breaches involving health care information have become increasingly prevalent in recent years, and such breaches seem to be continually growing in scope and magnitude. In the April 14, 2015, issue of JAMA, the *Journal of the American Medical Association*, three California researchers led by Dr. Vincent Liu (hereinafter Liu et al.) sought to more fully understand the scope and characteristics of recent data breaches and their impact on the health care industry. Liu et al. used data provided by the Department of Health and Human Services to look at all data breaches between 2010 and 2013 that affected the unencrypted protected health information of at least 500 individuals and were reported by entities covered under the Health Insurance Portability and Accountability Act (HIPAA). Liu et al.'s findings included the following:

- 949 total data breaches were reported between 2010 and 2013, with the annual number of breaches increasing from 214 in 2010 to 265 in 2013;
- 29.1 million records were affected by the 949 breaches, although certain records may have been involved in more than one breach;
- A breach was reported in every state, the District of Columbia, and Puerto Rico;
- Six breaches affected more than one million records each;
- 32.7% of breaches involved a portable electronic device or laptop, while 22.3% of breaches involved paper records;
- Theft (58.2%) was the leading cause of breaches, followed by unauthorized data access or disclosure (14.8%), and loss or improper disposal of data (11.1%);
- Hacking or information technology incidents were responsible for 7.1% of breaches; and
- 28.8% of breaches involved an external vendor.

Although Liu et al. cautioned that these findings likely underestimate the scope and characteristics of recent data breaches due to limitations in the underlying data, the findings are sufficient to provide a number of lessons for health care entities. As Liu et al. observed, the majority of data breaches were caused by criminal activity, with theft being the leading cause of data breaches. The findings also reiterate the importance of appropriate security practices by business associates, as nearly one-third of the breaches involved an external vendor.

Interestingly, 22.3% of the breaches involved paper records, and only 7.1% occurred due to hacking or an IT incident, a reminder that while hacking incidents receive significant publicity, health care entities must also be aware of security threats to non-electronic records. However, these findings likely under-represent the threat posed by hacking, as hacking can instantly expose huge amounts of data and be particularly difficult for health care entities to detect (and thus report). For example, the study did not include recent data breaches involving Community Health Systems and Anthem Health Insurance that collectively affected tens of millions of records and were allegedly the result of sophisticated hacking attacks. Regardless, Liu et al.'s findings reinforce the need for health care entities to be proactive in recognizing data security threats and implementing effective security protections.

– Conor O. Duffy

HIPAA

Pharmacy Settles HIPAA Investigation for $125,000

On April 22, 2015, the Office for Civil Rights (OCR) entered into its first HIPAA violation settlement in 2015. The settlement requires Cornell Prescription Pharmacy, a small pharmacy located in the Denver area to pay the OCR $125,000 and adopt a corrective action plan to implement policies and procedures and train employees on HIPAA.

The allegations against the pharmacy stemmed from a report by a Denver news outlet that documents containing health information of 1,610 patients were disposed of in an unlocked open container on the pharmacy's premises.

The OCR stated "[R]egardless of size, organizations cannot abandon protected health information or dispose of it in dumpsters or other containers that are accessible by the public or other unauthorized persons."

This is not the first settlement the OCR has obtained for the improper disposal of paper records. It is another reminder to health care organizations to check their policies and procedures and training regarding the proper disposal of paper records, including shredding.

– Linn Foster Freedman

ENFORCEMENT + LITIGATION

Objections To Radioshack's Sale of Customer Data Cause Static In Advance of Auction

Uncertainty will hang over the upcoming bankruptcy auction of RadioShack's intellectual property, franchise infrastructure, and customer data pending resolution of an ongoing struggle between RadioShack and several states' attorneys general concerning the proposed sale of customer data. As previously reported, RadioShack plans to auction personally identifiable information (PII) collected from more than 70 million customers. The State of Texas (joined formally or informally by 35 other states) objected to the sale citing several of RadioShack's own privacy policies which prohibited the sale of PII. RadioShack withdrew the PII from its prior auction, but has scheduled a new auction which would include PII.

In light of the prohibitions in RadioShack's privacy policies, Texas has argued that the sale of PII runs afoul of section 363(b)(1)(B)(ii) of the Bankruptcy Code because it "would violate applicable non-bankruptcy law" and Texas's Deceptive Trade Practices Act. Broadcasting a clear signal that it will continue to press its objection to the sale of PII, Texas unsuccessfully asked that the bankruptcy court require bidders to allocate their proposed purchase price for the PII so that judicial disapproval of the transfer of PII will not necessarily unravel the totality of a bid for RadioShack's other assets.

The bankruptcy court's order establishing bid and sale procedures indicates that RadioShack will engage in post-auction mediation with Texas and any successful bidder for the PII (if the bidder is willing to mediate). The order also sets dates for depositions concerning the sale of PII telegraphing that the fight over the issue will continue should mediation fail. Objections to the sale of PII are likely to be heard at the bankruptcy court's May 20, 2015, hearing to consider and approve a sale to the high bidder, so stay tuned.

– Steven J. Boyajian, Patrick Birney, and Mike Enright

FCC Cites Three Companies For Its Unwanted Robocalls

On May 4, 2015, the Federal Communications Commission (FCC) cited three companies, Call-Em-All LLC (Call-Em-All), Ifonoclast Inc. (Ifonoclast) and M.J. Ross Group Inc. (M.J. Ross) (Ifonoclast and M.J. Ross conduct business as Phonevite and PoliticalRobocalls.com), for their unwanted robocalls, threatening statutory fines of up to $16,000 per violation if the violations of the Telephone Consumer Protection Act (TCPA) don't cease. All three companies made robocalls to consumers' cell phones using both autodialers and prerecorded messages without first obtaining prior express consent from the consumers as is required by the TCPA. Each company was provided 30 days to respond to the FCC's citation.

Call-Em-All supplies its clients with a robocalling service wherein it sends prerecorded messages to its clients. Call-Em-All's clients include employment staffing firms; nonprofits such as schools, churches and sports leagues; and clients with political or commercial messages. Call-Em-All was previously investigated by the FCC back in 2012. Phonevite and PoliticalRobocalls.com offer services similar to that of Call-Em, and were also questioned by the FCC in 2012 for its questionable telemarketing practices and potential violations of the TCPA. Owner of PoliticalRobocalls.com, Moses Ross, said, "This effort by the FCC, I'm sure, is clearing out bad apples from the industry, so in that sense, I applaud it." We will keep you updated on these companies' response to the FCC's citation and the actions they each take within the next 30 days.

– Kathryn M. Sylvia

DRONE PRIVACY

Florida Passes Drone Surveillance Bill To Protect Personal Privacy

On April 28, 2015, the Florida State Legislature passed SB 766, or better known as the Freedom from Unwarranted Surveillance Act, which permits commercial drone use, but bans the use of drones for the surveillance of private individuals without their prior consent.

Specifically, the bill states that "a person, a state agency or a political subdivision [is prohibited] from using a drone to capture an image of privately owned real property or of the owner, tenant, occupant, invitee or licensee of such property with the intent to conduct surveillance without his or her written consent if a reasonable expectation of privacy exists."

But what does that mean? Well, the bill specifies that “a person is presumed to have a reasonable expectation of privacy on his or her privately owned real property if he or she is not observable by persons located at ground level in a place where they have a legal right to be.” The bill does not include an exception for law enforcement; law enforcement is required to obtain a warrant unless exigent circumstances exist, like a terrorist attack. However, there are exceptions for property tax valuation; inspection of electric, water, and natural gas utilities; aerial mapping; and cargo delivery, IF the drone and its operator are in compliance with Federal Aviation Administration regulations.

The bill is expected to be signed into law by Republican Gov. Rick Scott who is an advocate for consumer privacy. We will keep you posted.

– Kathryn M. Sylvia

DATA PRIVACY

Senate Democrats Offer Consumer Privacy and Protection Act of 2015

Senate Democrats, led by Senate Judiciary Committee Ranking Member Patrick Leahy of Vermont, introduced legislation on April 30, 2015, directed to online consumer privacy and data protection. The Consumer Privacy and Protection Act of 2015, one of multiple proposals before Congress this year, requires companies storing sensitive personal or financial information on 10,000 or more U.S. customers in a twelve month period to provide notice of security breaches affecting customers within thirty days. Of note, the proposed legislation protects not just personal identifying and financial information (such as driver’s license and credit card numbers), but also password-protected digital photographs, videos, and communications. Interestingly, while the Act would supersede state laws mandating less stringent data security practices, stronger state laws would not be preempted. As the Act would not impose a national standard for notice following a data breach, opposition to the legislation will likely focus on the challenges businesses face complying with state-by-state notice requirements. We will continue to monitor the various legislative proposals that could affect covered businesses.

– Benjamin C. Jensen

To get more thoughtful and timely discussions of legal news and perspectives on various issues relating to data privacy and security, subscribe to our *Data Privacy and 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 and Security Team.

© 2015 Robinson & Cole LLP. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission. This document should not be considered legal advice and does not create an attorney-client relationship between Robinson+Cole and you. Consult your attorney before acting on anything contained herein. The views expressed herein are those of the authors and not necessarily those of Robinson+Cole or any other individual attorney of Robinson+Cole. The contents of this communication may contain attorney advertising under the laws of various states. Prior results do not guarantee a similar outcome.