January 28, 2016

Today is National Privacy Day. What are you doing to celebrate? Here at Robinson+Cole, we are dedicated to educating and providing counsel to our clients on data privacy and security issues today and throughout the year. Happy National Privacy Day!

DATA BREACH

Centene Announces Search for Missing Hard Drives Containing PHI of 950,000 Individuals

Centene Corporation, a health insurer headquartered in St. Louis, announced on January 25, in a press release that it is undertaking an "ongoing comprehensive internal search for six hard drives that are unaccounted for in its inventory of information technology (IT) assets."

The press release states that the hard drives contained the names, addresses, dates of birth, Social Security numbers, member ID numbers, and health information of members who received laboratory services between 2009 and 2015.

Centene is notifying the affected individuals of the loss of the hard drives and is offering free credit and healthcare monitoring. It stated that it will continue to search for the hard drives, but they are unaccounted for at this time.

Two points: health care entities may want to consider whether full Social Security numbers should continue to be included in all of the data it receives and stores on an individual—do you really need the entire SSN on that hard drive; and second, full encryption of data at rest. If this information had been encrypted, it could not be viewed, stolen or used.

— Linn Foster Freedman

Wendy's Investigating Potential Credit Card Breaches

Wendy's may be the latest in a number of companies with Central Ohio operations that have suffered data breaches in recent years. On January 27, Wendy's announced that it hired a cybersecurity firm to investigate claims of a possible credit card breach at some of its locations. Initially, the company was notified by its payment industry sources that unusual activity was occurring on payment cards after they were used at certain Wendy's locations. While Wendy's has not completed its investigation, the breaches may have occurred late last year.

It is too soon to tell whether the breaches have been contained, how long they occurred, or how many stores were affected. However, the reports of unusual activity came from financial institutions in the Midwest and on the east coast.

Wendy's, which is based in Ohio, has approximately 6,500 franchise and company-operated restaurants in the United States and 28 countries worldwide. Most of the U.S. stores in operation are franchises.

— Kathleen E. Dion

ENFORCEMENT+LITIGATION

Facebook Biometric Case Dismissed

We previously reported about a proposed class action suit against Facebook for alleged violations of the Illinois Biometric Information Privacy Act. Facebook moved to dismiss the case for lack of personal jurisdiction.

On January 22, 2016, the Judge agreed with Facebook and dismissed the case stating that the plaintiff failed to allege that Facebook knew Illinois residents would upload photos to Facebook and tag individuals in the photos.

Further, the Judge stated that Facebook only operates an interactive website that is available to those who participate and doesn't target residents of a particular state or aim its conduct at the state.

This is a significant precedential holding relating to the Illinois biometrics statute, but Facebook faces a similar proposed class action case in California. Similarly, Shutterfly was unsuccessful in having the biometrics case against it in Illinois dismissed. We will continue to watch these cases closely.

— Linn Foster Freedman

SCOTUS Upholds Computer Fraud and Abuse Act Conviction

The Supreme Court of the United States held on January 25, 2016, that an executive of a shipping company who hacked into his former employer's computer system after he left the company was guilty under the Computer Fraud and Abuse Act (CFAA), despite the fact that the jury instructions were faulty.

The executive accessed the confidential information of his former employer after he left his employment. The former employer settled its civil claims against the executive for $10 million, but he was then prosecuted for criminal violations of CFAA.

After he was convicted, he appealed, arguing that the jury instructions were improper. SCOTUS rejected his argument, particularly because the defendant "did not dispute that we was properly charged with conspiracy to obtain unauthorized access or that the evidence was sufficient to convict him of the charged crime…"

— Linn Foster Freedman

CYBERSECURITY

Ukranian Cyber Hacker Pleads Guilty

Sergei Vovnenko, a Ukranian hacker, pleaded guilty last week in federal court in Newark, New Jersey to aggravated identity theft and conspiracy to commit wire fraud by using more than 13,000 computers to steal log-in information and credit card data. He faces a mandatory sentence of two years in prison and will be sentenced on May 2, 2016.

The allegations against Vovnenko are that between September 2010, and August 2012, he participated in a conspiracy to hack computers to steal user names and passwords for bank accounts and steal debit and credit card numbers through a botnet infected with malware known as "Zeus."

A related story is that Vovnenko was alleged to have been involved in a plot in 2013, to have heroin sent to Brian Krebs' home, and call police when they arrived to nail the unsuspecting Krebs. Well, I am a big fan of Brian Krebs. Check out his blog, Krebs on Security. Krebs followed the user "Fly," secretly gained access to his forum (where he learned about the plot), and exposed him. Which "likely contributed to his arrest and guilty plea." One for the good guys.

— Linn Foster Freedman

Spear-Phishing Campaigns Continue to Infiltrate Critical Infrastructure

The Department of Homeland Security's Industrial Control Systems Cybersecurity Emergency Response Team (ICS-CERT) has reported that critical infrastructure systems in the United States experienced a 20 percent increase in cybersecurity incidents in 2015. ICS-CERT responded to 295 incidents involving critical infrastructure in 2015.

The good news is that the industry that is the most targeted—Energy—had a 42 percent decline in attempts to infiltrate. The bad news—the critical manufacturing sector experienced an increase in cyber-attacks, particularly through spear-phishing campaigns. This illustrates the importance of employee training on spear-phishing and other social engineering schemes.

— Linn Foster Freedman

FireEye Acquires iSight Partners for $200 Million

Cybersecurity firm FireEye (owner of Mandiant forensics unit) has announced that it has acquired iSight Partners for $200 million, which boosts the two well-known cybersecurity firms' ability to provide additional cybersecurity offerings. The deal closed on January 14, 2016.

— Linn Foster Freedman

Is Point-of-Sale Drone Registration Next? Retailers Say No Way

In the first 30 days of drone registration, nearly 300,000 owners have registered their drones. The Federal Aviation Administration's (FAA) small drone user registration has sparked much debate, and now, the FAA is considering a change in their regulations to require immediate registration upon purchase. This point-of-sale registration would force retailers to become part of the drone registration process. The Retail Industry Leaders Association (RILA) believes that "customers' personal information will be better protected by ensuring retailers are not unnecessary middlemen in the process."

Specifically, the RILA expressed its concerns for consumer privacy, "In most instances, point-of-sale registration will require checkout clerks to ask customers to reveal personally identifiable information while standing in the checkout line in order to input the information into a registration system. This creates privacy concerns for consumers reticent about revealing personal information in such a public forum." Many individual retailers have commented that they would oppose this type of registration as well.

On the other hand, the FAA's concerns grow with the number of drones entering the skies; in 2015, there were over 600 drones spotted near airports and 13 cases in which drones interfered with fighting wildfires.

The FAA's rule is only an interim rule so expect much more debate and discussion of the issues that are currently 'up in the air.'

— Kathryn M. Rattigan

SOCIAL MEDIA

Oklahoma and Virginia Become Newest States to Consider Social Media Legislation

The list of states that have passed social media legislation is getting longer. Early next week, Oklahoma will become the latest state to consider social media legislation (along with approximately 23 others) to prohibit employers from asking employees or applicants to provide them with their social media account passwords and from being forced to access their social media accounts with their employer present.

Legislation was introduced in mid-January in Virginia that would prohibit public and private colleges and universities from requiring students to disclose their passwords to school officials.

The Uniform Law Commission is scheduled to vote in July 2016, on model social media legislation that would include prohibition of employers' access to employees' information and colleges and universities to access students' social media accounts.

— Linn Foster Freedman

INFORMATION GOVERNANCE

Preparing for a Sharepoint 2016 Migration

Many organizations are considering an update to their existing SharePoint environment in 2016. This is largely due to new functionalities being offered with SharePoint 2016, especially if the organization is still running SharePoint 2010 or later. With that said, a well thought out migration strategy is key to the

success of this project.

Let's consider five things organizations can do to prepare for a SharePoint 2016 migration.

Perform a Content Audit

The main purpose of a content audit is to identify any outdated or unimportant content to leave behind when moving to the new environment. By doing this, organizations will be sure to only migrate the content that is most important.

Consider Existing Security Permissions

Organizations most likely have a well thought out layer of security permissions already integrated into its existing SharePoint environment. So, it's crucial that the same level of security and access groups migrate over to the new environment. An automated migration approach will, more often than not, respect existing security permissions. Conversely, a more manual approach will require much more attention to be sure the same level of security is met. In addition, this may be a good time for the organization to revisit existing permissions and amend them as necessary.

Hardware and System Requirement

Creating a fresh SharePoint 2016 farm may require that the organization update its hardware and system requirements. The official hardware requirements can be found under "System Requirements" on Microsoft TechNet.

Must Have Sharepoint 2013

It's not possible to upgrade from SharePoint 2010 directly to SharePoint 2016. Organizations must upgrade to SharePoint 2013 first. After upgrading to 2013, organizations could either use one of the many migration tools on the market or perform the upgrade themselves. That decision will depend largely on existing knowledge resources and budget requirements.

Hybrid Cloud Option

In order to take advantage of the new cloud features in 2016, such as OneDrive for Business, organizations will need to really understand what information (if any) can't be moved to the cloud. That answer will largely depend on the legal and audit requirements in the organization's jurisdiction.

As discussed, there are many things organizations can do today in preparation for a migration to SharePoint 2016. Organizations that plan ahead now, surely will avoid much heartache down the road as well as set themselves up for a successful migration experience.

— James Merrifield

PRIVACY TIP # 19

Social Media Account Hackings and Social Engineering

My Facebook account was hacked on Friday night. We were skyping our daughter, when she put the screen of her phone up to the computer screen and said, "Mom, why are you friending me?"

I looked at the friend request and immediately noticed that it was from LinnFoster Freedman with no space between my first and middle names. It looked very odd to me, but apparently, did not look unusual to many of my Facebook friends.

I posted on my wall in all caps that no one should accept the friend request and should block that user. Several of my savvy friends reported the impersonator to Facebook and the impersonator's profile was taken down within 10 minutes and Facebook emailed me to let me know that the profile was taken down. It was a flurry of activity.

I am not an active participant on Facebook, but look at it and post things every once in a while. Sorry, my friends, but I really don't follow every move you make. If my daughter hadn't told me about the fake friend request, I would not have figured it out for days. Once I found out, I did some research and learned that it is a frequent problem.

Unfortunately, many of my Facebook friends fell for the fake and it prompted me to write this post.

This was a classic social engineering scheme. When imposters can get into Facebook accounts, they have access to all sorts of information that they might not otherwise be privy to, and can amass that information with other information to get a clear picture of people they are targeting.

So what are we to do? Some would say don't participate in any social media accounts. That is a personal decision. If your social media account has been hacked, change your password immediately to stop any unauthorized access.

When someone friends you, look at the request closely. When I looked at the request and noticed that there was no space between my name, it looked funny and I knew it was fake. So did my daughter. But it was close enough that others missed the nuance. So look closely and make sure it doesn't look strange. Also, obviously, make sure you actually know the person. And before you automatically say "yes," check to see if you are already a friend of that person. If you are, it is suspect and you should reach out to the person to ask why they are sending another request.

Of course, I want to know how my account was hacked and I have sent Facebook several questions that I want answered about the incident. Facebook has not replied. I have been told by others that I will get a response when "H-E-Double hockey sticks freezes over." I guess you get what you pay for. But isn't my data that is being mined (including photos) worth at least a response?

— Linn Foster 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.