May 19, 2016

DATA BREACH

FDIC Reports Five "Major" Data Incidents to Congress

The Federal Deposit Insurance Corporation (FDIC) reported on Monday, May 16, 2016, that it had experienced five "major incidents" involving the disclosure of taxpayers' personal information since the last incident we reported on last month involving 44,000 records.

A "major incident" is defined as involving more than 10,000 records. The reported incidents all involved FDIC employees who "inadvertently" downloaded over 10,000 taxpayers' information along with personal files when they left their employment with FDIC.

The FDIC reported that it obtained affidavits from each of the departed employees attesting that they did not share the information with others. Hopefully, the FDIC was able to retrieve the taxpayer information so it is no longer in the possession of these individuals and are limiting employees access to taxpayers' personal information going forward.

The FDIC stated that it is launching new procedures to protect data, including software "to force encryption of portable devices."

— Linn Foster Freedman

Newest Ponemon Study Released on Health Care Data Breaches

The Ponemon Institute has recently released its Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data. The study has included business associates for the past two years. The study included information received from 91 covered entities and 84 business associates, which is a good determinate of the risk of breaches caused by third parties.

The estimates of the costs associated with data breaches to the health care industry are up to $6.2 billion. The survey results include that up to 90 percent of the health care organizations in the study suffered a data breach in the past two years, and almost half of them suffered more than 5 data breaches during that same period. Although most of the breaches involved data of less than 500 individuals, the message is clear: health care organizations continue to be a target.

The results of the study show that the average cost of a data breach for a health care organization is $2.2 million. The average cost of a data breach to a business associate is more than $1 million. According to the study, “Despite this, about half of all organizations have little or no confidence that they can detect all

patient data loss or theft." And although health care organizations have increased their budgets for data security, most of them still don't have a sufficient budget to combat the problem.

The leading cause of data breaches in the health care sector is criminal attacks. This is evidenced by the recent incidents of malware and ransomware that have been in the news. According to the results of the study, 50 percent of health care organizations said the cause of the data breach was a criminal attack, and 13 percent said it was caused by a malicious insider.

41 percent of business associates confirmed that a criminal attacker caused the data breach and 9 percent said it was due to a malicious insider.

The primary forces behind the data breaches were ransomware, malware, and denial-of-service attacks. Secondary causes include employee negligence, mobile devices, cloud service providers, and BYOD. These internal issues and employee actions were identified as the cause of a data breach by 36 percent of health care organizations and 55 percent of business associates.

The bottom line? Health care organizations are still at a high risk for cyber intrusions and employee neglect that can cause a data breach and may wish to consider continuing to invest in data security measures and employee training to combat the continuing issue of cyber intrusions and employee actions that lead to a data breach. Vendor management and employee training are key to risk management of these issues.

— Linn Foster Freedman

LinkedIn Admits that 2012 Data Breach Affected 177 Million Users' Data

A LinkedIn data breach in 2012 supposedly exposed 6.5 million LinkedIn users' hashed passwords. LinkedIn announced yesterday (May 18, 2016) that, in fact, it impacted more than 177 million user accounts and that the information was posted online. Therefore, as of today, LinkedIn is forcing individual users affected by the 2012 breach to reset their passwords.

It is being reported that a hacker is selling the e-mails and passwords of the LinkedIn users for $2,000.

Regardless of whether you receive notification from LinkedIn that you were affected, it might be wise to change your password now.

— Linn Foster Freedman

CYBERSECURITY

New Study Confirms That 9 out of 10 Businesses Have Experienced a Hacking Incident in the Last Year

Hartford Steam Boiler released a study on May 17, 2016, that states that nine out of ten businesses have experienced at least one hacking incident in the past year, which represents a 21 percent increase since 2014.

The survey of risk managers showed that 64 percent of risk managers admitted that their organization had experienced more than six hacking incidents in the past year, which is a 32 percent increase over

2015.

Nonetheless, businesses continue to embrace Internet of Things devices for improved productivity and efficiency, despite the risks associated with the devices. According to the study, 56 percent of business say they will implement or plan to implement IoT devices, while only 28 percent felt they were safe for business use.

Surprisingly, the study showed that the risk management strategies that those surveyed are implementing include an increase in encryption technology, but a decrease in intrusion detection/pen testing, and a significant decrease in employee education (only 12 percent use employee education programs, down from 24 percent last year.)

Employee education is an essential part of a risk management program. The decrease in employee education programs is concerning, and companies may wish to reevaluate that strategy. Although encryption is key to a risk management program, it is not the panacea.

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

Win for Businesses—for Now: Supreme Court Rules in Favor of Spokeo in FCRA Litigation

Today, the U.S. Supreme Court issued a ruling in *Spokeo Inc. v. Robins*, marking a win for businesses—*for now*.

In a prior post, we discussed Spokeo, Inc.'s (Spokeo) request to the Supreme Court to overturn the February 2014 ruling from the Ninth Circuit that revived the Fair Credit Reporting Act (FCRA) lawsuit filed against Spokeo by Thomas Robins. Robins alleged that Spokeo violated the FCRA by falsely reporting his financial, marital, and educational status (for the better, we might add). He was portrayed as wealthy, married, and a graduate degree recipient when in fact he was unemployed and struggling financially.

By a 6-2 vote, the Supreme Court said, "We have made it clear time and time again that an injury in fact must be both concrete and particularized…. A 'concrete' injury must be 'de facto'; that is, it must actually exist." The Supreme Court further said, "[H]arm does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right. Article III standing requires a concrete injury even in the context of a statutory violation."

This ruling means that the case will go back down to the Ninth Circuit for determination as to whether Robins was harmed or not. The Supreme Court specifically said, "This does not mean, however that the risk of real harm cannot satisfy the requirement of concreteness." This leaves room for lower courts to continue exploring the issue of harm in consumer litigation. And as we have seen from many cases across the country, there is no one decision in this regard. Additionally, the Supreme Court failed to provide any insight as to whether consumers can even bring a class action suit over so-called "statutory violations." We will keep an eye on the case as it heads back to the Ninth Circuit and let you know the outcome.

— Kathryn M. Rattigan

ATM Skimmer Pleads Guilty in RI Federal Court

Skimming continues to be a problem for ATM machines, and law enforcement continues to try to combat the problem. Skimming devices are attached to credit and debit cards and ATM machines in order to intercept debit and credit card information and PIN numbers as they are being entered by an individual. The skimmers then re-encode the information on fake debit and credit cards, use the cards to purchase items, and defraud the unsuspecting victims.

The U.S. Attorney in Rhode Island recently announced that a skimmer admitted that he conspired to attach skimming devices on ATM machines in Rhode Island and Connecticut and pleaded guilty to charges that he was involved in a skimming scam where 1,392 individuals' debit cards were compromised between January 1, 2015, and April 4, 2015. The skimming scheme resulted in a loss of $709,598. The skimmer will be sentenced on July 20, 2016.

To protect yourself from skimming devices, whenever you pay with a credit or debit card, grab the top of the payment machine and jiggle it to make sure it doesn't come off. If it does, it is probably a skimmer, and you should alert the store or bank. If it doesn't, it should be safe to use.

— Linn Foster Freedman

HEALTH INFORMATION

FDA Issues Guidance on the Use of EHRs in Clinical Investigations

The U.S. Food and Drug Administration just issued draft guidance on the Use of Electronic Health Record Data in Clinical Investigations for comment within the next 60 days.

The guidance is intended to assist all parties associated with clinical research with the appropriate use of electronic health records in FDA-regulated clinical investigations, which, in general, includes information from medical devices.

The draft guidance, which is nonbinding, would apply to the use of electronic health information in prospective clinical investigations involving human drugs and biologic products, medical devices, and a combination thereof.

Comments to the draft guidance should be submitted by July 16, 2016.

— Linn Foster Freedman

DRONES

FAA Announces More Drone Detection Testing at JFK Airport

The Federal Aviation Administration (FAA) announced this week that it will be expanding its research on how to detect "rogue" drones near airports. The FAA will join forces with other government agencies and academic partners to experiment with new drone detection technology at JFK Airport in New York. FAA senior advisor on drone integration, Mark Gibson, said, “We face many difficult challenges as we integrate rapidly evolving UAS technology into our complex and highly regulated airspace. This effort at JFK reflects everyone’s commitment to safety.” The FBI and Department of Homeland Security will also participate in these tests. The FAA plans to continue using the FY 2016 Appropriations Law to fund its

interagency strategy to evaluate and assess drone detection systems at several different airports throughout the rest of the year. As the detection system gets better, safety in the skies may also too.

— Kathryn M. Rattigan

TECHNOLOGY

Is CaaS the Solution for Privacy and Security in the SaaS World?

Companies are under tremendous pressure to reduce IT costs. Cloud and Software as a Service (SaaS) offer significant potential cost reductions through the use of shared infrastructure and standardized software offerings. However, there are often significant concerns if the service or application stores or processes personally identifiable information, important intellectual property, other sensitive information, the criticality of the system, or whether the solution opens avenues into a company's core systems.

A new application of the technology software "containers" offers a potential approach that may reduce many of the risks in current SaaS offerings, while allowing for more security and control. Containers as a Service (CaaS), primarily using software from the open source Docker Project, allows for software to be embedded in a container and delivered to a party, without regard to the recipient's particular infrastructure. This would allow the purchaser of the software to choose between different models of software operation, from full-hosted cloud, to on-premises behind a firewall.

As more software is developed using the Docker framework, there will be increased choices for software deployment both inside and outside an organization. This will require software providers to develop new pricing models that better reflect the resources necessary to support a customer and customers to understand the shifting risk issues that result from licensing and running software in a new manner. New licenses need to be developed, and the license compliance implications of adding existing software to containers must also be addressed. Using Docker security and trust services would provide an extra layer of protection, as would requiring SDLC controls and a SOC2 report as minimal requirements.

— Richard M. Borden

GUEST AUTHORS

I am pleased and privileged to be an adjunct professor teaching privacy law at Roger Williams University Law School. Every year, I offer my students the opportunity to submit a blog article that is of interest to them to be included in the R+C *Data Privacy + Security Insider*.

This year, we had an abundance of material to choose from, as there was a lot of activity in data privacy and security! I am pleased to share the thoughts of these bright and talented students and know that they will serve our profession well.

— Linn Foster Freedman

Think You're Covered? Think Again

Commercial General Liability policies (CGL) typically do not include data protection loss coverage, although some insurers offer additional data protection endorsements. Normally those additional endorsements only cover data losses caused by physical damage. That means, if your employee

damages a server that stores client or patient data, that could trigger coverage. It would not, however, cover the same employee accidently releasing client/patient data or loss from ransomware or other malware. In a recent case the parties were in dispute over whether the insurance company had a duty to defend the insured against class-action allegations that the insured posted patient data on the Internet. In April, a federal appeals court in Virginia upheld a lower court ruling that a CGL policy *may* cover the underlying data breach. This opposes two state court cases in New York and Connecticut that held that CGL policies *generally* do not require a duty to defend in the instance of cyber-attacks.

Cyber insurance policies (CIP) don't guarantee coverage for data breaches either. CIP underwriting requires risk management professionals to have a plan, a method, and an understanding of what coverage is needed for the organization. Although it varies by company, most CIPs require this analysis be provided with an organization's own privacy policy in its application for insurance and bind it with the coverage. This was the case in *Columbia Cas. Co. v. Cottage Health Sys*., where Columbia issued its' CIP to Cottage Health Systems. After a breach resulted in the loss of 32,500 patients' information by Cottage Health, Columbia denied coverage when it found that the insured misrepresented its information privacy practices and security in 10 instances on its application.

The message should be clear: don't rely on insurance for data breach protection. It is important that an entity has a privacy policy and security measures in place and in force.

— *Alfonso Nardi*

Important Issues Are Yet to be Corrected in the Right to be Forgotten

The recognition by the European Union of a "Right to be Forgotten" caused much controversy, but is seemingly making progress. The right, which entitles Europeans to petition data controllers to prevent harmful information about them from appearing in web searches, has been criticized for opening the door to bad-faith claimants to silence legitimate journalism. Recently, an international effort has produced the Oblivion Framework, capable or sorting hundreds of claims for merit in mere seconds. However, these advances ignore a much larger problem regarding the Right to be Forgotten; the EU has yet to announce any meaningful regulations respecting what information is actually protected.

This is problematic for multiple reasons. Unclear guidance from the EU regarding what is entitled to be forgotten places large data controllers like Google in the unenviable position of making educated guesses about how to comply with the law. This is greater cause for concern. Google's process for vetting claims involves a number of experts and officials from across the data privacy field, but how it works remains unknown. This current system allows data controllers to self-regulate, unless an individual with the time and resources to press major litigation forces the case to the EU Court of Justice.

This is not to say that the Right to be Forgotten is intrinsically flawed. Similar processes are used to routinely seal criminal records in expungement proceedings. Yet, in these cases the requirements and procedures are clearly defined by statute. With clear guidance, individuals in the EU could tell when and how to they are entitled to protect their information and move on from the ghosts of their pasts.

However, until the EU provides such guidance, Europeans only have a Right to be Forgotten to the extent that data controllers are prepared to give them one.

— *Michael Ferron*

PRIVACY TIP #38

Employees Still Careless—Don't Be That Employee

According to a study by Softchoice, 1-in-5 employees still keep their passwords in plain sight (like a Post-it Note on their desk or in the top drawer of their desk—now that's original), have accessed work files from a device that was not password protected, and have lost devices that were not password protected. Really?

The study also found that employees continue to download apps without letting their IT department know, which puts their organization at risk. Even more surprising to me is that employees continue to use cloud-based applications like Google Docs and Dropbox for work, which may not be approved by their organization. According to Softchoice, employees "continue to display reckless technology habits that put their employers at risk."

I don't know about you, but I don't want to be "that" employee. I don't want to be the one who gets that phone call that accuses me of doing something "reckless." I am thinking you don't want to be that employee either.

The study shows that younger employees are more likely to download cloud apps that put their company at risk and that, although most employees respect their IT department, that didn't stop them from breaking the policies and procedures of the organization. That is a sobering statistic that we all need to pay attention to and reverse. Give your IT guys a break—they are working hard.

According to the Verizon 2016 Data Breach Investigations Report, data security training for employees is essential. Employees need to be aware of company policies and abide by them. So employers, step up that training of your employees. And employees, step up that vigilance to help protect your employer and your company data. You really don't want to be "that" employee—do you?

— Linn Foster Freedman

UPCOMING EVENTS

Authors' Events

In addition to their legal practice and involvement with the blog, our Data Privacy + Security Team regularly serve as presenters at topic-related seminars, and participate on panels that discuss developments in the area. Several speaking engagements at scheduled events are featured below:

- May 20 – Annual Massachusetts Bar Association Health Law Conference (Linn F. Freedman & Kathryn M. Rattigan)
- June 7 – The Quorum Initiative Cyber Intrusions event in New York City (Linn F. Freedman)
- June 8 – The Quorum Initiative Cyber Intrusions event in Washington D.C. (Linn F. Freedman)
- June 22 – National Scholarship Providers Association in Rocky Hill, CT (Linn F. Freedman)
- June 23 – MCLE: Data Security 2.0: The Cloud, Mobile Devices & Encryption Webcast Panel (Kathleen M. Porter)
- July 11 & 12 – Seventeenth Annual Institute on Privacy and Data Security Law (Kathleen M. Porter)

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.

Boston | Hartford | New York | Providence | Stamford | Albany | Los Angeles | Miami | New London | rc.com

Robinson & Cole LLP