July 21, 2016

CYBERSECURITY

Symantec Releases "Ransomware and Businesses" Report

Symantec Corp released its annual "Ransomware and Businesses" Report this week outlining the increasing sophistication of ransomware attacks. Individuals continue to be the primary target of ransomware attack, as they usually have the weakest security measures. Although the health care industry has clearly been targeted recently, the report states that the service and manufacturing industries had significant attacks at 38 percent and 17 percent respectively.

According to the report, the hackers have a "gold rush" mentality now that is boosting their confidence and is providing incentive to find more and more sophisticated techniques and the request for higher payments.

Symantec stated, "A growing number of gangs are beginning to focus on targeted attacks against large organizations…that can potentially infect thousands of computers, causing massive operational disruption and serious damage to revenues and reputation."

Message? Ransomware will continue to increase and be a problem for organizations in the coming months and years as the hackers are getting paid and continue to be incentivized to find more and more sophisticated techniques. Organizations may wish to continue to focus on combatting ransomware in their organization, as it is not going away.

— Linn Foster Freedman

Black Hat Reports Increase in Cybersecurity Concerns

The 2016 Black Hat Attendee Survey was published in advance of the 2016 Black Hat Conference. Not surprisingly, the respondents to the survey conveyed an increased concern regarding security breaches versus 2015. An alarming 72 percent of respondents believe it likely that their organizations will have to deal with a major data breach in the year ahead. Of those, 15 percent had "no doubt" that they will need to respond to a major security breach, and 25 percent said it was "very likely" that they will face a major security breach. Startlingly, 74 percent of respondents said that they did not have enough staff to face the threats they expect to encounter. Even more startling, 67 percent of respondents stated that they themselves do not have enough training to do their jobs. There is also a significant gap in the vulnerabilities the respondents face, with social engineering, including phishing, and sophisticated attacks targeting the organization being the top two, and where security professionals are spending their time and resources—measuring risk, managing compliance with industry and regulatory requirements, and

troubleshooting vulnerabilities. The results of the survey paint a picture of organizations that are struggling to protect information and systems but do not have the resources or guidance to provide the appropriate protections. There are federal, state, and municipal rules on fire safety. Every company has a sophisticated fire prevention, response, and remediation plan. There are governmental and independent fire agencies. A call to 911 brings prompt and sophisticated help. Insurance companies play a major role in remediation assistance. It is time to treat cyber risk like we treat fire risk.

— Richard M. Borden

Brown Cybersecurity News Podcast: Professor Linn Freedman on Cybersecurity Opportunities for Professional Women in Non-Tech Sectors

Linn Freedman is as senior as it gets in cybersecurity. In addition to her EMCS faculty position, Linn is a partner at the law firm Robinson+Cole, where she chairs the firm's Data Privacy + Security Team. Yet her background is not in computer science or a technical field. In this brief podcast she talks about the rich career opportunities for women in cybersecurity who, like her, might lack a technology background. Find out how she used her work in health care in the Office of the Rhode Island Attorney General as a stepping-stone to an exciting career in cybersecurity and learn about the industry's need for a broad range of experts across policy, privacy and technology.

• Listen to the podcast.
• View the podcast transcript.
• Learn more about the Brown University Executive Master in Cybersecurity.

HIPAA

Oregon Health & Science University Pays $2.7 Million Penalty for Data Breaches

Oregon Health & Science University (OHSU) has agreed to settle alleged HIPAA violations involving two separate data breaches with the Office for Civil Rights (OCR) for $2.7 million.

In the span of three months in 2013, OHSU experienced two reportable data breaches, which triggered investigations by the OCR.

The first occurred when an unencrypted laptop containing the PHI of 4,022 patients was stolen from the vacation property of a physician in Hawaii.

The second occurred when physicians used a cloud storage service to share a spreadsheet that contained PHI of 3,044 patients. However, no business associate agreement was put in place prior to using the cloud service and sending the PHI, which, according to the OCR, "put the data at risk."

This guidance from the OCR, along with the hefty fines, provides strong incentives to encrypt laptops and put effective processes in place for business associate management. Informing physicians and staff about HIPAA requirements and the use of cloud vendors and other third-party service providers is key so they understand the risks and are aware of the business associate management program of your entity.

— Linn Foster Freedman

HHS: Ransomware Attacks Likely HIPAA Breaches in Absence of Encryption

On July 11, 2016, the U.S. Department of Health & Human Services (HHS) issued a Fact Sheet that provides guidance on (i) how HIPAA Security Rule compliance can assist health care organizations combat ransomware attacks and (ii) the applicability of HIPAA's Breach Notification Rule to ransomware attacks. This guidance is particularly timely due to the recent proliferation of ransomware attacks (see previous posts here and here), which Office for Civil Rights (OCR) Director Jocelyn Samuels characterizes as "one of the biggest current threats to health information privacy."

Ransomware

The Fact Sheet defines ransomware as "a type of malware (malicious software)… [whose] defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid."

HHS notes that ransom is often demanded in a cryptocurrency, such as bitcoin or ether, to reduce the likelihood that the hacker can later be identified.

Security Rule

According to HHS, compliance with the Security Rule can help entities prevent malware attacks and mitigate damage caused by such attacks. The Fact Sheet mostly reiterates fundamental Security Rule requirements in the context of a malware attack, including the importance of a comprehensive risk analysis, implementation of security measures informed by the risk analysis, having a data backup plan as part of an overall contingency plan, security incident response procedures, and appropriate security training for workforce members. The Fact Sheet emphasizes that the Security Rule only establishes minimum security requirements, and health care organizations are encouraged to adopt more stringent measures.

Breach Notification Rule

The Fact Sheet also addresses applicability of the Breach Notification Rule to ransomware attacks. HHS states that when electronic protected health information (ePHI) "is encrypted as a result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired" by an unauthorized person, and therefore the ePHI was "disclosed" in violation of the Privacy Rule.

Interestingly, HHS uses the phrase "a breach has occurred" in the Fact Sheet but also acknowledges that, while an impermissible disclosure is presumed to constitute a breach under the Breach Notification Rule, that presumption can be overcome by demonstrating that there is a low probability that PHI has been compromised based on a risk assessment. The Fact Sheet includes specific guidance on conducting a comprehensive risk assessment after a ransomware attack, but the above excerpt could suggest that HHS will likely be skeptical of claims that there is a low probability that PHI was compromised by a ransomware attack. This interpretation is supported by OCR Director Jocelyn Samuels's above-cited blog post, which states in pertinent part that "[t]he guidance makes clear that a ransomware attack usually results in a breach" under the Breach Notification Rule.

Finally, the Fact Sheet provides an important reminder regarding the benefits of encryption. Because the Breach Notification Rule only applies to "unsecured" PHI, HHS affirms that, as long as ePHI has been encrypted in accordance with HHS encryption guidance such that it is no longer unsecured, a ransomware attack involving such encrypted ePHI would not constitute a reportable breach.

— Connor O. Duffy

ENFORCEMENT + LITIGATION

Scottrade Data Breach Class Action Case Dismissed for Lack of Standing

We previously reported that Scottrade was hit with a class action case within 24 hours of notifying customers of a data breach [view related post]. According to the complaint, the data compromised included the names, addresses, telephone numbers, Social Security numbers, and work history of customers.

The case against Scottrade was dismissed last week as the plaintiffs failed to show that they were harmed by the breach and, therefore, had no standing to sue Scottrade. The case was dismissed without prejudice by the judge, which means that the plaintiffs can later file an amended complaint.

The judge found that the claims of increased risk of identity theft, the cost of monitoring their accounts, the invasion of privacy and deprivation of the value of their personal information were speculative, as the plaintiffs were unable to show that their information has been used to commit identity theft or fraud and that the court would have to "engage in considerable speculation about the hackers' possible intentions and future actions" to be able to determine whether they will suffer harm in the future.

— Linn Foster Freedman

Ex-Cardinals Scouting Director Sentenced to Serve Time in Jail for Astros Database Hacking

Back in January, we wrote about the ex-Cardinals scouting director pleading guilty to hacking the Houston Astros database. This week, Christopher Correa, former scouting director and director of baseball development, was sentenced to 46 months in prison for unlawfully accessing computers and emails of the Houston Astros. Correa admitted to accessing a protected computer and using the passwords of former Cardinals employees who moved to the Astros. Correa accessed the Astros' database, known as "Ground Control," to view private communications about prospective baseball players. The database included contract information, scouting reports and other proprietary analyses of every player in Major League Baseball. Also, Correa accessed information weekly Astros' scouting digests, draft strategies and notes about trade discussions. Correa must pay $279,038 in restitution to the Astros. Each of the five counts had the potential for five years in prison, but the prosecutors agreed to allow Correa to serve the time concurrently.

— Kathryn M. Rattigan

Major League Baseball Investigating Cardinals-Astros Hacking

Promptly following the sentencing of Christopher Correa [see related post] on July 18, 2016, Major League Baseball Commissioner Rob Manfred announced that Major League Baseball (MLB) is looking further into the hacking incident involving Houston Astros emails and information on players for evaluating potential draft picks.

According to Manfred, he has asked the MLB's Department of Investigations to investigate the facts and to request information from law enforcement so he can take "appropriate action."

The commissioner has the power to investigate any action that "is not in the best interest of the national game of baseball" and can take punitive action against any MLB club, owner, employee, or player who is involved.

— Linn Foster Freedman

DRONES

Utah Votes to Let Authorities Disable Drones Near Wildfires

This week in Salt Lake City, lawmakers approved a bill that would allow Utah authorities (that is firefighters or law enforcement) to disable and down drones if they are being flown too close to wildfires. Governor Gary Herbert said, "This summer, wildfires in the state have become significantly worse due to drones interrupting air operations. It is dangerous and completely unacceptable, and this legislation takes steps to ensure that our emergency management personnel are safe and empowered to do their jobs effectively." While this bill would allow the authorities to shoot down a drone if it was interfering with containment of a wildfire, because the drones are flying so high, it would be difficult to do; however, the use of jamming signals to crash the drones is more likely. Authorities would be able to use the jamming technology to disable a particular drone without affecting other aircraft or technology. A violation of this new law could result in a maximum punishment of 15 years in prison and $15,000 fine if the drone causes a firefighting aircraft to crash.

— Kathryn M. Rattigan

DATA SECURITY

ATM Vulnerability – Banks Beware!

It is said that a chain is only as strong as its weakest link. Often the same is said for an organization's data privacy and security defensives. Could it be that the ubiquitous ATM machine is the weak link to the banking system? On Thursday, July 14, IBSintelligence.com reported that in Taiwan thieves, possibly using a cellular device, hacked into 41 separate ATM machines and made off with the equivalent of approximately $2.2 million. Taiwan's largest bank was forced to freeze transactions on 1,000 of its ATM machines, which represents about four percent of the country's ATM population. All 41 hacked machines were manufactured by the same vendor, Wincor Nixdorf. Wincor Nixdorf has stated it is aware of the thefts and is working with police and the bank on the issue. It further stated that the vulnerability exists irrespective of manufacturer. Three different types of malware have been identified as the tools used to commit the thefts.

The hacking and stealing from ATM machines is on the rise in Asia, and Fortune.com, reporting on the same story on Sunday, July 17, wrote that in May several individuals stole approximately $13 million in less than three hours from ATMs in Japan. Several arrests have been made in the Taiwanese incident, and a little over half of the money was recovered from a hotel room.

With almost a half a million ATM machines in the United States, the question is when, not if, will we see similar large heists in the U.S. and what effect will it have on the ATM banking industry? Citigroup is currently working with ATM maker Diebold on two new models, one that requires a retina scan for authentication and a second that requires an application running on the customer's smartphone.

— Sean Lawless

DATA PRIVACY

I-9: Ways to Avoid Identity Theft

I. Compliance can begin during the interview – Ask applicants:
Do you have authorization to work in the U.S.?

II. Let candidates know in the offer letter/application that they will need to complete the Form I-9 as a condition of employment.
Language for offer letter: Your employment is conditional upon your successful completion of the Form I-9 verifying both your identity and authorization to work in the U.S.

III. Have an experienced/trained person be responsible for completing the I-9 forms with the employee.

IV. Question the validity of documents which seem suspicious.
Permanent Resident Cards should no longer include "INS" or "Immigration Naturalization Services" anywhere on them. Cards should only have forward-facing photos and not three quarter view photos. They are called Permanent Resident Cards now and not Resident Alien Cards. If you notice any of these issues, it is a red flag to question the card.

Driver's licenses can be difficult to verify, as each state has its own document, and they can be changed/updated frequently. If you have reason to suspect a license may be fraudulent, it is acceptable to look for a sample license at the state's website for assistance. Some states/sites have helpful information online, including the following:

California: https://www.dmv.ca.gov/portal/wcm/connect/e090f7ec-64bc-4e87-afc8-e66895903b37/dl627e.pdf?MOD=AJPERES
Texas: https://chadhasty.wordpress.com/2009/04/23/texas-redesigns-your-drivers-license/
Connecticut: http://www.ct.gov/dmv/cwp/view.asp?a=805&q=379684

V. Keep copies of documents but do not make and keep copies of documents you don't need
If you have a List A document, you should only have a copy of the List A document and not extra documents from List B and/or C. If you don't have a List A document, you would need copies of both the List B and List C documents.

VI. Review the I-9 to verify that it is completed correctly and perform self-audits.

VII. Consider proper transmission and storage of the I-9.
As sensitive personal information is contained on the Form I-9, careful employers will be cautious about where the I-9 is stored and where it might be duplicated. Faxing or emailing Forms I-9 (unless the email is encrypted) can create risks of inadvertent disclosure. Be cautious about an unsecure digital copy that could be created in a scanner or on someone's email account. Paper I-9 forms will be more secure if stored in a secure space under lock and key.

This post was co-authored by Megan Naughton, Josh Mirer, Lauren Sigg, and Jennifer Shanley. This post is also being shared on our Manufacturing Law Blog. If you're interested in getting updates on developments affecting manufacturers and distributors we invite you to subscribe to the blog.

PRIVACY TIP #44

The Flashlight App's Collection of Your Data

When you start needing longer arms to read restaurant menus in the candlelight, you might consider downloading a flashlight app to use with your reading glasses.

But before you download it, first be aware that your iphone or Android have flashlights automatically installed. If you download a flashlight app, just be aware of what data that flashlight app is collecting.

Some flashlight apps ask for access to your location-based services, your contacts, your photos, your camera, and the microphone. Do you want the app developers to have access to all of that data just so you can read that menu?

Some flashlight apps also may request your permission to install other apps and make your ability to uninstall the app difficult.

As an individual, read the privacy policy of the app, including the flashlight app before you automatically click "I agree." Be aware of what data you are giving the app developers, including the flashlight app and make an educated decision on whether your use of the app is worth the sharing of all of your data.

— 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 area. Following, are several upcoming speaking engagements:

- August 10 – NSPA Regional Meeting in Washington, D.C. (Linn F. Freedman)
- 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)

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.