August 25, 2016

DATA BREACH

Eddie Bauer Latest Victim of Point-of-Sale Compromise

Eddie Bauer announced on August 18 that it is the latest retailer who has become a victim of a "sophisticated" cyber intrusion that has compromised all of the cash registers in the 350 Eddie Bauer stores throughout the U.S. and Canada.

The malware compromised the point-of-sale system and the names, credit and debit card numbers, security codes, and expiration dates of every credit and debit card used at an Eddie Bauer store from January 2, 2016, through July 17, 2016.

Eddie Bauer, like other retailers in the same boat, is offering identity theft protection services for those customers who used a credit or debit card at any of its stores during that time frame.

— Linn Foster Freedman

KPMG Survey Finds That Shoppers Care about Retail Data Breaches

On the heels of Eddie Bauer's notification of a cyber intrusion affecting all of its retail stores in the U.S. and Canada, KPMG has released a study showing that almost one-fifth of respondents to a survey said they would avoid a retailer that was a target of a successful cyber intrusion, even if the company remediated the damages caused by the hacker.

In response to the survey, 33 percent said they would stop shopping at the store for at least three months following the compromise for fear that their personal and financial information may be exposed. They also said that they would avoid the retailer until its leadership publicized a plan to prevent future attacks.

This translates into approximately 19 percent of the retailers' customer base.

Sounds like worrisome statistics for retailers, doesn't it? Surprisingly, the same survey found that 55 percent of senior cybersecurity executives in the retail sector admitted that they had not invested in cybersecurity over the last twelve months.

The numbers outlined in the KPMG survey may cause those cybersecurity executives to lose sleep but is good evidence for retailers to reconsider and bolster cybersecurity efforts. It is clearly affecting the bottom line.

— Linn Foster Freedman

CYBERSECURITY

Locky Ransomware Continues to Hit Health Care Entities

FireEye Labs has reported that the Locky ransomware continues to hit the health care industry hard and has increased in the month of August.

Although the telecommunications, manufacturing, and aerospace/defense industries are also being targeted with Locky ransomware, the health care industry is being attacked with greater frequency and intensity.

The health care industry should be on alert for an increase in phishing schemes, unfamiliar emails, attachments, and links, and employees should be on high alert for any suspicious emails, which is the most common way Locky is introduced into a system. Employee training is key in providing employees with education around ransomware so entities do not become victims of these increased attacks.

— Linn Foster Freedman

Cybersecurity Risks to the Manufacturing Sector

The 2016 Manufacturing Report by Sikich finds that there has been a progressive growth in cyber-attacks in the manufacturing sector. This is consistent with the most recent IBM/X-Force Research 2016 Cyber Security Intelligence Index, which notes that the manufacturing industry represents the second most attacked industry, just behind health care.

Manufacturing companies often don't believe that they are targets because they do not hold vast amounts of consumer data. Therefore, they do not concentrate on cybersecurity and remain vulnerable. These two reports show that the risk of a cyber-attack is high and real to the manufacturing sector.

According to the Sikich report, the risks to the manufacturing sector include the following:

- operational downtime
- physical damage
- product manipulation
- theft of intellectual property and sensitive data

These reports are a dose of reality to the manufacturing sector that it is under attack, and the threats and risks of cyber intrusions are real and are not dissipating. Addressing these risks and the potential devastating consequences is critical for any company in the manufacturing sector.

— Linn Foster Freedman

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.

Hackers Dubbed 'Ghoul' Targeting Industrial Businesses across the Globe

Researchers at Kapersky Labs say they have uncovered an industrial hacking scheme that they have dubbed “Operation Ghoul” that has hit 130 organizations in 30 countries. Kapersky says Operation Ghoul targets bank accounts and intellectual property of small- to medium-sized industrial businesses using an off-the-shelf, commercial malware program known as Hawkeye that is capable of recording keystrokes, monitoring browser and email data, and stealing FTP server credentials.

— Linn Foster Freedman

The Goal of Gender Equality in Cybersecurity

I have the privilege of teaching the Privacy Law class at Roger Williams University School of Law (RWU). It is a required course for the school's Joint Masters in Cybersecurity/Juris Doctor program, which is, to my knowledge, the only joint program offered by a university and law school in the U.S.

A recent statistic states that only about 25 percent of law schools in the country offer a privacy law class, let alone any substantive classes in cybersecurity. Based upon my practice and experience, such offerings should be a high priority for educators from grade school through advanced degree programs. Why? Because, based on several governmental studies, there is a dearth of qualified individuals in the United States that can provide expertise in information technology (IT) or cybersecurity, both for the government and private industry.

In Rhode Island, Governor Raimondo has set a goal for all students to be offered computer science classes, which is a commendable start. But businesses in the U.S. are recruiting qualified IT and cybersecurity professionals from other countries every day because they can’t fill open positions domestically.

You needn’t look past the front page of the newspaper every morning to find news of yet another cyber intrusion in which a company has become the victim of a hacking or data breach. RWU Law has placed itself ahead of the national curve by offering classes that are relevant to fulfilling the needs of businesses in the U.S. and also providing its students with the knowledge and experience they'll need to find rewarding jobs when they graduate and for the rest of their careers.

Last year, cybersecurity and data breaches continued to be one of the highest risks facing all industries. Preparing young professionals to combat these risks will provide them with an exciting career, and businesses with much-needed expertise.

My pitch here is that higher education should be responding to the needs of all industries, as RWU Law is doing—but we also need to actively recruit women to the fields of IT and cybersecurity. And we need to collectively have the goal of ensuring gender equality in these male-dominated fields.

National statistics show that, although women make up 57 percent of the workforce, only 25 percent of the technology sector is comprised of women. Even more depressing is that only 20 percent of chief information officers at Fortune 250 companies are women. Research also shows that the pipeline of women in IT executive jobs is dismal.

Why? I am convinced it is because the word “cybersecurity” conjures up images of computer science, cryptology, encryption, and coding, and these terms are inherently intimidating to girls and women. We have to figure out a way to make these fields more enticing to women. I try to encourage women into

these fields, but a collective effort would be much more effective.

Another obstacle may be that women are not being paid equally in these fields. Although IT and cybersecurity continue to grow as industries, and salaries are increasing in these sectors, a recent Healthcare Information and Management Systems Society (HIMSS) survey shows that the gender pay gap in IT salaries is widening.

How can this be in 2016? According to the HIMSS study, in 2015, women in IT made only 78 percent of what their male colleagues made. It further states that "…where men's salaries increased at a compound annual growth rate (CAGR) of 1.16 percent, women's salaries only grew by a CAGR of 0.79 percent." This pay gap actually widens at the executive level, with women in senior or executive management roles only making 85.5 percent of what their male colleagues earn.

This must stop. How will we be able to recruit women to IT and cybersecurity if they aren't paid equally as their male counterparts? How will we be able to maintain a diverse working population in these sectors if there are gender-based pay discrepancies even wider than in other fields? We have been battling these issues for decades and the battle must continue.

As we did in the past with getting more and more girls and women involved in the fields of engineering, math, and STEM, we must now band together as educators to get ahead of the needs of businesses and recruit and retain women in the fields of IT and Cybersecurity. And we must ensure that women are paid on par with their male counterparts and have the same opportunities to work in these very exciting fields.

The security of our nation literally depends on us getting it right because right now hackers from other countries are stealing companies' intellectual property, individuals' personal information, and governmental secrets.

We need a diverse and effective workforce in IT and cybersecurity to protect these interests, and RWU Law is leading the way.

— Linn Foster Freedman

This is a reposting from the Roger Williams University School of Law blog http://law.rwu.edu/node/11846

DRONES

The Small Drone Rule (Part 107) is effective on August 29, 2016

Part 107 of the Federal Aviation Regulations (or the Small Drone Rule) applies to nonhobbyist small unmanned aircraft (UAS) commercial operations of all drones under 55 pounds. The final rule will go into effect on August 29, 2016. The Federal Aviation Administration (FAA) recently released a guide and a short video for UAS operators to use in preparation for the required aeronautical knowledge test, which is now an integral component to the commercial operation of UAS and in obtaining a required remote pilot certificate.

To qualify for the certificate, the individual must pass the aeronautical knowledge test at an FAA-approved knowledge testing site or have an existing nonstudent Part 61 pilot certificate.

However, even if the individual has a Part 61 license, they must take a FAA UAS online training course

and have completed a flight review in the prior 24 months.

Additionally, Part 107 sets forth specific operating requirements (and restrictions). Read a summary of those requirements here.

— Kathryn M. Rattigan

EPIC Challenges FAA's Final Drone Rule for Lack of Privacy Protections

The Electronic Information Privacy Center (EPIC) filed a complaint against the Federal Aviation Administration (FAA) this week alleging that the final drone rule (Part 107) fails to include privacy regulations. EPIC claims that it has made previous attempts to ensure that the FAA "adequately addresses the privacy implications of drone deployment" to no avail. EPIC was told by the D.C. Court of Appeals earlier this year that it could not seek review of the FAA's drone rule until it was a final order. Now, with the final rule issued on June 28, 2016, and the effective date set for August 29, 2016, EPIC is reigniting its fight again. EPIC's complaint asks the court to vacate the FAA's final rule and remand to the FAA for further consideration and proceedings on the issue of privacy matters.

— Kathryn M. Rattigan

ENFORCEMENT + LITIGATION

Florida Court Holds Budget Request Forms and Activity and Service Fee Records Not "Educational Records"

On August 11, 2016, a Florida state court judge held that the University of Central Florida Board of Trustees (UCF) must produce budget request forms and activity and service fee database records to Knight News, Inc. (KNI) in response to KNI's public records request. The records indicate the amount of money paid to each student for services rendered or for reimbursement of expenses incurred in his or her duties as a student government officer. Initially, UCF produced the records but redacted student names. UCF claimed that the students' names were "educational records" and thus exempt from disclosure under the Family Educational Rights and Privacy Act (FERPA) and Florida law.

The court held that the requested records were subject to complete disclosure under Florida's public records law because they did not fall within FERPA's definition of educational records. Under FERPA, educational records must be kept in a central location or folder that a parent or student could easily request. UCF did not maintain these records in a manner contemplated by FERPA of educational records. If a student or parent requested a student's educational records, the budget request forms and A&S fee database records would not be included in the production merely because the student's name was listed on these documents. Accordingly, these documents were not educational records under FERPA or Florida's public records law. Furthermore, the court held that members of the student government implicitly consented to the dissemination of this information under Florida law.

— Kathleen E. Dion

PRIVACY TIPS

Privacy Tip #49 – Use a Passphrase Instead of a Password

I love to train employees on data privacy and security. It tends to be rather entertaining as I can tell crazy stories about real life scenarios about data breaches or compromises. The stories are quite beneficial, as most employees say "I would never do that!"

One of my favorite stories to tell, as it is a common mistake and people in the audience always nod when I tell it, is of an employee of a vendor who downloaded the names, addresses, dates of birth, and Social Security numbers of all of the employees of a company onto a laptop and took the laptop home to work on the data over the weekend.

The employee's apartment was broken into over the weekend and the laptop was stolen. I got the call on Monday morning asking what they needed to do. My first question was "Was the laptop encrypted?" The answer was "No, but it was password protected." The employee couldn't remember the password so wrote it on a yellow sticky note and stuck it in the inside of the laptop. Ugh. So the thief got the laptop, the password, and all of the employees' personal information, including their Social Security numbers. That, folks, is a reportable data breach.

The point is that passwords are a pain in the you know what. No one can remember a complex password, and they have to be changed every 60 days. It continues to be a thorn in all employees' sides.

My favorite password tip is to use a passphrase instead of a machination of different letters and numbers. For instance, "Myfavoritecolorisred!" My favorite color IS red, and I can remember that when I sit down at the computer. It has a capital letter, is long and complex, and has a symbol at the end. Most security guys approve of it. And if I can remember my password, I won't be dumb and write it down on a piece of paper and put it in my top drawer (really, do you think that is such a trick?) or on a sticky note on my desktop.

I have been giving this tip for years, and now a new study from Carnegie Mellon University has confirmed the tip by saying it is a best practice.

So when you get to work tomorrow, change your crazy password that you can't remember to a passphrase that you can remember. But don't use the same one at work as you use at home. Use another phrase that you can remember from your personal life, like "Mydog'snameisRover". Um, but don't use your real dog's name as hackers can figure that out from your Facebook page…

— 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.