KNOW GREATER VALUE™

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Cyber Roundup – July 2018

By Thomas J. DeMayo, Principal, Cyber Risk Management

Here we go again. We do not lack for material in our monthly report on cyber shenanigans. Clearly, individuals and businesses are vulnerable to any manner of cyber hacking and fraud. So, why not call on us to assess your risk and help protect against such threats? Our assignments are tailored to our client and their needs; our professionals are highly qualified; and, our approach is systematic. It's your business, your call.

Key Cyber Events

The following is a rundown of what happened during the month of June 2018. We welcome your comments, insights and questions.

- **MyHeritage, a genealogy and DNA testing company, disclosed that a security researcher found a file on a private internet server that contained the e-mail addresses and hashed passwords of approximately 92 million users.** A hash of a password is similar to encryption in that in serves to protect the password at rest. In response to the breach, MyHeritage is requiring all users to reset their password. Full details have yet to be released.

- **Verizon, Sprint, AT&T and T-Mobile announced they will stop selling customers' phone location data to third parties.** This move was in response to an investigation by U.S. Senator Ron Wyden that identified that law enforcement agencies were able to obtain the information from the third parties to track individuals without user consent or proper warrants. Unrelated to this, a few days after this story broke, the Supreme Court ruled that police must get a search warrant before obtaining location data from the mobile carriers or similar services.

- **Ticketfly, a major event ticket distribution service, announced that they suffered a breach that resulted in the theft of 26 million personal records including information such as users' names, phone numbers, e-mail and home addresses.** No payment information was compromised. The hacker responsible for the breach had originally informed Ticketfly of the security vulnerability and demanded a ransom of one bitcoin (at the time roughly $7,500) to reveal the vulnerability and help correct it. Ticketfly did not respond to the request and the hacker defaced the website and breached the information.

- **Ticketmaster reported a breach that potentially affected the payment details of millions of users.** While the breach is still under investigation, Ticketmaster is blaming an external third party supplier, Ibentia, that provides and hosts a customer support chat application on Ticketmaster's website.

- **The Atlanta police department, in the wake of the Ransomware attack in March that crippled the city, informed the public that years' worth of dashcam videos had been lost and could not be recovered**. The lost footage could compromise ongoing cases, such as DUI cases. This should serve as a reminder that every business should have procedures in place to audit their backup routines and ensure all necessary data is protected.

- **Cryptocurrency mining malware is up 629% in the first quarter of 2018, according to a report issued by MacAfee Labs**. The report notes that the Company has seen five new cryptocurrency mining malware samples every second. Based on other industry reports, the malware being designed is not target specific and infects all different types of devices including smart phones and Macs.

- **Exactis, a marketing and data aggregation firm, exposed a database containing approximately 340 million personal records.** The leak was identified by a security researcher. At a staggering two terabytes in size, the database contained such information as names, phone numbers, addresses, personal characteristics, interests, habits and the number and gender of their children. In total, the database had 400 potential variables regarding characteristics of individuals. It is not known if any criminals accessed or obtained the information; however, if they did, this information would allow for very targeted phishing attempts.

- **FastBooking, a hotel booking software provider for more than 4,000 hotels in 100 countries, reported a security breach.** The breach consisted of guest personal information inclusive of payment information. The breach was recognized on June 14th when company staff identified malware on the server. The breach occurred through the exploitation of a vulnerability in a web application that allowed access to the back-end systems containing the data. The full details of the affected hotels and number of users has not yet been released.

- **PageUp, an Australia-based human resource software as a service company, reported a breach as a result of a malware attack.** Given the nature of the data the company handles, a treasure trove of personal information could have been affected. The full details of the breach have yet to be released. Every business has personal information on their employees. As part of any cyber risk assessment, the protections afforded to employee personal information should be a primary consideration.

- **The Office for Civil Rights issued a $4.3 million HIPAA violation penalty against The University of Texas MD Anderson Cancer Center.** The penalty is the result of the Center failing to encrypt patient data on portable devices including a laptop and removable media. Although the Center had policies requiring encryption and identified the lack of encryption as a high risk item during their risk assessment, they failed to properly enforce and address the risk.

- **WiSpear, a Cyprus-based surveillance company, claims to have developed a van that can infect Apple and Google phones from a third of a mile away.** The van, selling at a cost of $3.5 – 5 million, works by using long range WiFi interception technology that forces the smart phone devices to connect to the van's WiFi access point. Once connected, the van can either steal data or infect the devices.

Contact Us

Thomas J. DeMayo, Principal, Cyber Risk Management
CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE

PKF O'Connor Davies, LLP
665 Fifth Avenue, New York, NY, 10022
212.867.8000 or 646.449.6353 (direct)
tdemayo@pkfod.com

www.pkfod.com

About PKF O'Connor Davies

PKF O'Connor Davies, LLP is a full-service certified public accounting and advisory firm with a long history of serving clients both domestically and internationally. With roots tracing to 1891, nine offices in New York, New Jersey, Connecticut and Maryland, and more than 700 professionals, the Firm provides a complete range of accounting, auditing, tax and management advisory services. PKF O'Connor Davies is ranked 29th on *Accounting Today*'s 2018 "Top 100 Firms" list and is recognized as one of the "Top 10 Fastest-Growing Firms." PKF O'Connor Davies is also recognized as a "Leader in Audit and Accounting" and is ranked among the "Top Firms in the Mid-Atlantic," by *Accounting Today.* In 2018, PKF O'Connor Davies was named one of the 50 best accounting employers to work for in North America, by *Vault*.

PKF O'Connor Davies is the lead North American representative in PKF International, a global network of legally independent accounting and advisory firms located in over 400 locations, in 150 countries around the world.