Cyber Roundup – February 2019

By Thomas J. DeMayo, Principal, Cyber Risk Management

So, you've been lucky so far. Neither you nor your business has been compromised by cyber crime. Maybe Shakespeare's warning [which basically applies to most life circumstances] can be your guide: ***Better three hours too soon than a minute too late*.** Good advice from a guy who died over 400 years ago and never had a smartphone.

As you will see from this month's edition of ***Cyber Roundup***, in the blink of an eye, you can become a victim. Now's the time to contact us and get a cyber check-up.

Key Cyber Events

The following is a rundown of what happened during the month of January 2019. We welcome your comments, insights and questions.

- **Four breaches occurred as a consequence of improperly configured and unsecured internet-accessible databases:**

    - A database containing approximately 7 million call logs, 6 million text messages, documents and passwords was identified by a security researcher. The database belonged to a California-based communications provider, Voipo. The company has stated that although the database was exposed, no evidence was found to indicate that a data breach had occurred. The company is continuing to investigate the matter.

    - A database belonging to the Oklahoma Security Commission exposed a treasure trove of sensitive data. The data consisted of FBI confidential case files on investigations over the past seven years, 17 years of archived e-mails, health records, and thousands of Social Security numbers. The issue is currently under investigation.

    - A database belonging to the AIESEC (Association Internationale des Etudiants en Sciences Economiques et Commerciales) exposed the information on approximately 4 million young intern applicants. AIESEC is an international not-for-profit with the mission of empowering young people to make a positive impact on society. The organization will inform all impacted individuals.

    - A database containing millions of documents relating to mortgages and loans was identified as exposed. The database belonged to Ascension, a data and analytics company located in Texas. When Ascension was notified of the discovery, it concluded that their vendor, OpticsML, was responsible for mishandling of the data. As you can imagine, the mortgage and loan related documents contained W-2s, tax forms, Social Security numbers, name, address, phone numbers, etc. Everything needed to facilitate identity theft or W-2 fraud. W-2 fraud is when the cyber criminals file tax returns on the victim's behalf to obtain a refund.

PKFOD Comment: Many businesses — whether for-profit or not-for-profit — handle sensitive data to support their mission. While some have heeded the warnings and have taken a proactive stance in defending against the cyber threat, many have not and remain reactive. In the breaches noted above, these events weren't the result of a sophisticated hack, but a breakdown in internal controls that resulted in misconfigurations and, ultimately, data exposure. While we often

associate breaches with a hacker, that often is not the root cause. Until a fundamental shift occurs and cyber/data security is no longer viewed as a business expense, but a key enabler in supporting the business and its mission, these issues will continue to occur. If you need assistance in learning how to build a cyber security program that is proactive, effective, and a business enabler, please feel free to contact us.

- **A major security bug was identified with Apple FaceTime**. It allowed a caller to hear audio and see video from the target device without the recipient accepting or rejecting the call. The flaw is associated with Apple's Group FaceTime feature. Apple has disabled the feature in the interim until a patch is made available.

- **A U.S. judge has ruled that a person cannot be forced into using a biometric to unlock their device**. Judge Kandis Westmore, in presiding over a case in the U.S. District Court for the Northern District of California, ruled that forcing the use of a biometric [e.g. fingerprint, voice, iris, etc.] to unlock a person's device violates the Fifth Amendment against self-incrimination.

- **The City of Del Rio, Texas was the victim of a Ransomware attack, shutting down operations.** The City turned off all internet access to the City departments and prohibited employees from logging into their system as a precautionary measure. The City is still investigating the matter and has not yet reported if any personal data has been compromised.

  PKFOD Comment: As a Firm, we work with many municipalities. Unfortunately, many are still not getting the funding they need approved to proactively address the cyber threat, resulting in either nothing being done or the assessment being awarded to the lowest bidder who often is not qualified to perform the review. Until that changes, municipalities will continue to be actively targeted and victimized by the cyber criminals.

- **A group of U.S. senators called on the Federal Communications Commission (FCC) to investigate the major cellular providers and their practice of selling customer location data.** The major telecommunication providers, such as AT&T, T-Mobile and Sprint, have a practice of selling customer location data to third party aggregators. Once sold, it is continually resold, until eventually it ends up in the hands of bounty hunters and other individuals who should not have access to such personal data. Services exist on the black market that will locate a phone using a phone number for around $300. In response to this finding, Sprint, AT&T and T-Mobile all issued a statement that they would stop selling the data.

- **In another user location matter, the Los Angeles City Attorney's office filed a lawsuit against The Weather Channel for selling user location data collected through their mobile app.** The suit claims that The Weather Channel does not disclose in their privacy policy that they collect the user location data and subsequently sell it to third parties, ultimately misleading the consumers. Unfortunately, the collection and sale of location data has become a very valuable data set for advertisers, retailers, hedge funds and other industries looking to obtain valuable information into consumer habits. The next time you download an app, think twice before letting it know your location.

- **Apple removed a Facebook research app from the App Store over privacy violations.** Facebook, as part of market research, was paying people between the ages of 13 to 35 years up to $20 per month in exchange for downloading the app and granting access to the user's phone and web activity, inclusive of such personal data as messages and their location. Apple identified that Facebook did not submit the app to Apple's review process as required, but abused an Apple program that allows companies to create apps for internal purposes and testing only. Apple later suspended both Facebook's and Google's access to the program, when learning that Google also abused the program. While access has since been restored, Apple sent a clear message to the tech giants that privacy violations will not be tolerated.

- **The Cryptocurrency Ethereum Classic was the victim of a double spend attack worth 1.1. million.** A double spend attack is when a group of malicious miners obtain enough computational power to effectively alter the blockchain. In this attack, the miners were able to recover previously spent coins and transfer them to new entities under their control. In response to the attack, Coinbase, a cryptocurrency exchange, suspended all trading of Ethereum Classic. When it

comes to cryptocurrency, the more ethical miners, the more resistant the currency is to the double spend attack. This places the smaller and less popular cryptocurrencies at a greater risk.

- **A new strain of Ransomware was identified claiming to fund a fictitious charity for children with cancer after the payment is received.** To add legitimacy to the story, the cyber criminals utilized the images from various crowdfunding pages devoted to helping pay for medical treatments for children with cancer. Such an approach further demonstrates that the cyber criminals have no moral compass when it comes to the tactics they will employ.

- **A massive collection of approximately 2.2 billion breached usernames and passwords has been made available on hacker forums and file torrents.** Consisting of five different collections, dubbed Collection #1 and #2-5, the data has been compiled over time from various well-known breaches such as dropbox, linked-in, etc. While the data is relatively old, the risk lies in the fact that users have poor password habits, specifically using the same password across multiple sites and/or using predictable variations of the same password.

  PKFOD Comment: To help companies manage this risk, you may find value in our Dark Web Monitoring service, designed to help proactively identify these exposures and alert you when your business credentials are located for sale in the hacking community.

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, ten 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.