Cyber Roundup – October 2019

By Thomas J. DeMayo, Principal, Cyber Risk Management

Given the cyber misconduct reported for September alone we need to plan and devise ways to protect our cyber privacy and not wait to be victimized. Not only is it technical data that is being compromised, but cybercriminals have now found ways to use our human qualities – like our voice, finger prints, etc. – to exploit us for monetary rewards. We can work with you to help mitigate exposure to cybercriminals.

Key Cyber Events

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

- **As the bell rang for millions of students starting their school year in September, so did the alarm for ransomware attacks targeting those schools.** The Flagstaff United School District in Arizona suffered a ransomware attack impacting 15 of their schools. The District cancelled classes for a number of days to restore operations. Monroe-Woodbury Central School District in New York also delayed the start of their school year as it recovered from a ransomware attack.

Tom's Takeaway: While no business is immune from a ransomware attack, it is clear that cybercriminals have taken a significant interest in targeting municipalities and school districts. In a report by anti-virus vendor Emisoft, 68 municipal entities and 62 school districts have reported successful ransomware attacks in the first nine months of 2019. While we have said this in prior issues of *Cyber Roundup*, the municipal sector needs to embrace and fund their cybersecurity initiatives as a component of public safety and to ensure a safe and effective educational environment. Until this shift in philosophy is seriously adopted, municipalities and school districts will continue to be victimized by cyber threats.

- **Philip Capital Inc., a Chicago-based futures brokerage firm, was required to pay a settlement of $1.5 million by the U.S. Commodity Futures Trading Commission (CFTC) as a result of a cyber incident.** Philip Capital Inc. suffered a breach of their e-mail system in February of 2018 that resulted in the withdrawal of $1 million from a customer's account. CFTC specifically noted that the chief compliance officer was not familiar with the firm's technology and cyber security program.

Tom's Takeaway: When we work with compliance officers of financial institutions we often stress the importance that they understand the effectiveness of their cybersecurity program in mitigating their risks. All too often, the compliance officers rely too heavily on their IT department to manage and monitor their cyber program with little oversight. For many smaller financial institutions, they rely on an IT managed service provider. While it goes without saying that they should rely on their IT department or managed service provider on a day-to-day basis, the compliance officer must also monitor and understand the effectiveness of that program. A key component of that monitoring is independent IT audits and cyber assessments that are communicated directly to the compliance officer.

- **A new form of fraud has surfaced with the cyber criminals using artificial intelligence (AI) and voice technology to impersonate individuals.** *The Wall Street Journal* reported on an incident in which the CEO of an unnamed German company was impersonated using voice technology to trick the CEO of one their subsidiaries – a UK-based energy firm – into transferring $243,000. Based on the article, the CEO impersonator of the parent company called the CEO of the subsidiary requesting a payment be made to a Hungarian supplier immediately. Using the AI technology, the voice sounded like the German CEO, accent and all. The payment was made. The CEO of the UK firm became suspicious when a call was received later that day requesting another transfer.

Tom's Takeaway: This may be a new tactic to transfer funds; however, the solution to the problem remains the same. Any fund transfer must have an out-of-band verification process to known numbers and individuals.

- **A new scheme has been identified in the dark web by cloud security vendor, Armor, in which cyber criminals are selling discounted stolen cash in exchange for Bitcoin.** The transaction costs 10 to 12 cents on the dollar. While the buyer of the cash stands to make a considerable profit, they are also assuming the bulk of the risk by taking the cash.

- **As the states continue to adopt increasingly restrictive consumer privacy laws, the CEOs of technology powerhouses such as Amazon, AT&T, Dell, IBM, Walmart and others, issued an open letter to Congress.** They are calling for the enactment of a federal online privacy law that will preempt state privacy laws. This is an attempt to control a fragmented privacy landscape that could be confusing and costly to comply with.

Tom's Takeaway: While the tech companies clearly have a profit incentive to standardize the laws, I also believe that a single all-encompassing federal law is the best course of action. In a global economy with consumer data crossing state and country lines on a daily basis, it will be necessary to avoid the confusion and inequity that disparate laws may create.

- **User credentials of 36 million Poshmark customers are now circulating in the dark web for sale to cyber criminals.** Poshmark, which is an online clothing retailer, disclosed a breach of consumer data in August 2018 that had occurred in May of 2018. The breached data consisted of personal data inclusive of hashed user passwords. A hash of a user password is a scrambled version of the actual clear text password. The purpose of hashing a password is to protect it in the event of a breach. While a hash does provide a level of protection, it can be cracked and reversed to identify the clear text user password given enough time. Of the 36 million hashed credentials exposed, one million of those credentials have been cracked and are now circulating in the clear. Inevitably, the number of cracked credentials will increase over time. If you are a user of Poshmark, make sure that the password you used for Poshmark is not used for any of your other online accounts.

- **An Amazon AWS data center facility experienced a power outage that resulted in customer data loss.** The incident occurred at an Amazon AWS US-EAST-1 data center in North Virginia. Amazon did have backup generators; however, they also experienced a failure which resulted in equipment abruptly shutting down. Once power was restored, hardware damage was identified on select equipment resulting in the loss of some customer data.

Tom's Takeaway: Many companies rely on a single robust data center to not only run their servers but also store their backups in the same location. While many of these data centers are built to drastically minimize the risk of going down and losing power, it is no guarantee. This incident further emphasizes the age old adage of not storing all your eggs in one basket.

- **Food delivery service, DoorDash, reported a data breach impacting 4.9 million customers, delivery contractors ("Dashers"), and merchants that signed up with the platform prior to April 5, 2018.** Exposed data includes name, address, e-mail, order history, phone number, and hashed passwords. Financial account numbers were not compromised. DoorDash has notified the affected users and has recommended that they reset their password.

- **Security researchers at Greenbone Networks performed a study that identified servers around the globe exposing approximately 24.3 million patient records from 52 different countries.** The data consisted of medical images, patient name, date of birth, attending physician, purpose of examination and – specific to 13.7 million U.S. citizens – their Social Security number. The images consisted of X-rays, CT and MRI scans. The researchers analyzed 2,300 medical archive systems around the globe and identified 590 were publically accessible with no security mechanism in place (such as a password) required to access the images.

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, eleven offices in New York, New Jersey, Connecticut, Maryland and Rhode Island, 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 2019 "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 2019, 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.