KNOW GREATER VALUE™

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Cyber Roundup – November 2018

By Thomas J. DeMayo, Principal, Cyber Risk Management

As we gather around the dinner table on Thanksgiving Day, we might all put away our smart phones, give Alexa some time off, and enjoy the "actual" (not "virtual") company of our family and friends. After dinner, we may use our fitbits to work off the calories, create our electronic holiday cards, catch-up on our fantasy football team, update our Facebook page, do some e-shopping or maybe Skype with those who were not able to make it for dinner. Information technology has taken us far from that first Thanksgiving Day almost 400 years ago. Before too long, robots may be preparing and serving our Thanksgiving meal.

When the euphoria of the perfect holiday dissipates, we need to confront the reality of cyber-crime. Here's where our *Cyber Roundup* steps in as the spoiler.

Key Cyber Events

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

- **Hacking forums in the Dark Web were identified offering Business E-Mail Compromise (BEC) as a service starting at $150.** The offering specifically targets accounting and finance departments. BEC — noted by the FBI as having resulted in $12 billion in losses since 2013 — is the tactic used by cybercriminals to spoof the identities of company employees, generally executives, to defraud the company, partners or customers of money. Once they gain access to the e-mail accounts, they will typically search for pending transactions in the hope of redirecting the funds or look for contract or payroll-related information. Armed with the necessary information, they will leverage the identity of the compromised account to begin issuing requests to steal funds. One of the many ways an attacker may gain access to a mailbox is by looking for existing breached credentials of the company or employee they are targeting. Cyber criminals know that account holders like to use the same password [or similar variations] across many websites. PKF O'Connor Davies offers dark web monitoring services which may benefit your organization.

- **In response to the ever-increasing BEC threat, the SEC released an investigative report cautioning public companies to consider cyber risk and threats when assessing and identifying accounting internal controls.** The SEC's report was based on the investigation of nine public companies that lost millions of dollars as a result of cyber fraud. Specific to the SEC's focus is the risk of BEC. The SEC Chairman Jay Clayton noted that "*Cyber frauds are a pervasive, significant, and growing threat to all companies, including our public companies. … Investors rely on our public issuers to put in place, monitor, and update internal accounting controls that appropriately address these threats*." The Chairman further stated that the report emphasizes that all public companies have obligations to maintain sufficient internal accounting controls and should consider cyber threats when fulfilling those obligations.

- **The town of West Haven, CT was the victim of a Ransomware attack.** The attack resulted in 23 servers being taken offline and disrupting day-to-day services. The town ultimately decided to pay the attackers demand of $2,000 in bitcoin. Fortunately, upon payment, access to the town's systems was restored.

- **In an unrelated incident, a North Carolina water utility, ONWASA, also suffered a Ransomware attack.** Although IT staff members identified the attack was occurring and took protective measures, the speed at which the Ransomware spread could not be contained.

Several key databases had been encrypted. The utility did not pay the Ransomware and is currently rebuilding. It is estimated it will take several weeks before all services are restored.

- **U.S. voter registration records for approximately 35 million individuals across 19 states were identified for sale on the Dark Web.** The records are currently being sold by state; however, all the states can be purchased for $42,200. The most expensive state — going for $12,500 — is Wisconsin, while the least expensive is Minnesota at a price tag of $150. The records consisted of information such as: name, address, phone number and voting history. In an effort at "customer satisfaction," the seller of the records is promising to provide updates to the records on a weekly basis.

- **A Maryland firm that handles political fundraisers, inadvertently exposed data and passwords to databases containing voter records.** The exposure was the result of an improperly configured internet accessible Network Attached Storage (NAS) device. Once access to the NAS was obtained, a spreadsheet of usernames and passwords to a database called NGP was further identified. NGP is a private database used by the Democratic Party. The accounts allowed access to voter records used for fundraiser campaigns.

- **An unknown cyber criminal launched an attack against consumer grade home routers to steal banking credentials.** The attacker targeted known vulnerabilities in the devices in order to modify settings that would result in users being directed to web sites under the attackers control when they tried to access their banking web portal. While the attack was initially targeting users in Brazil, the scope has expanded. This serves as a reminder to ensure that any internet-connected device you own must be consistently updated to protect against these types of attacks.

- **Cathay Pacific, a Hong Kong based airline, alerted that approximately 9.4 million customer records had been breached.** The breach consisted of sensitive information such as: customer names, date of birth, phone numbers, e-mail and physical addresses and passport numbers. The breach was first suspected in March and confirmed in May; however, the breach notification occurred in October. Given the length of time and the type of information impacted, this may trigger penalties from various governmental entities around the world, but specifically the EU as a result of the GDPR regulation that went into effect in May of 2018. Under GDPR, entities have 72 hours to report a breach. If you believe you may be impacted by the breach, you can visit the following link https://infosecurity.cathaypacific.com/en_HK.html to obtain additional information

- **FitMetrix, a fitness software company, exposed millions of customer records as the result of an unsecured Amazon Web Service (AWS) database.** The exposed information contained such details as: name, gender, e-mail address, birth date, phone numbers and health information including weight and height. The exposed database was identified by a security researcher that was searching the internet for databases of this type that were not secured. What is interesting is that upon identifying the database, the researcher also found a ransom note from a prior attempt of a cyber criminal trying to extort the company as a result of the same weakness. This demonstrates that the tactics used by cyber criminals are no different than those used by cyber security researchers, the question is, who can find it first.

- **The *2018 U.S. State of Cybercrime*, produced by IDG, a media, data and marketing services company, reported some interesting statistics as follows:**

    - 75% of cyber-attacks originate from outsiders. 25% are the result of insiders.
    - 39% of respondents noted that the cyber attacks from outsiders are the most costly.
    - The most common outsider attack vectors are:
        - Phishing – 53%
        - Malware – 50%
        - Spyware – 45%
    - The most common insider threats:
        - Employees being tricked by social engineering – 42%
        - Employees blending work and personal usage – 26%

The significant takeaway from this study is that employee education is key. A successful employee cyber awareness training program can account for all the threats noted in a core capacity. At PKF O'Connor Davies, we take a "people first" approach. By understanding the

employees, their habits, their strengths and their weaknesses first, we can then design and layer in processes and technology to minimize risk and drive performance.

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.