PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Cyber Roundup – February 2020

By Thomas J. DeMayo, Principal, Cyber Risk Management

Healthy **skepticism** can help avoid falling for phishing schemes and way-out-there data equipment/systems scams; **testing** can help ensure that the data system actually works and supports your company's stated policies and procedures; and, **knowledge** allows for expanding data enhancements and securing the necessary and appropriate hardware, the software and the data. It is hoped that incidents reported in *Cyber Roundup* provide you with helpful material so you can avoid similar events, and that our "takeaways" give you actionable information.

Key Cyber Events

The following is a rundown of what happened during the month of January 2020. We welcome your comments, insights and questions.

- **The Internet Crime Complaint Center (IC3) issued an alert notifying the public of cyber criminals leveraging false job openings to steal applicants' personal information.** To commit the fraud, the criminals will go as far as setting up fake websites to increase the perceived legitimacy of the opening. The criminals will conduct fake interviews and provide fake offers while requesting sensitive information, such as the individual's SSN or bank account number.

Tom's Takeaway: It is important that every person have a degree of skepticism when it relates to any electronic communications or circumstances that require the collection of sensitive personal information. Before you enter the information onto a form – whether paper or electronic – make sure the collector of that information is legitimate and has the proper controls to protect that information.

- **Amazon-owned home security camera provider Ring has made the headlines again as it reported having to terminate employees who improperly accessed the video data of Ring users.** In addition to terminating the employees, Ring has increased the limitations on the number of employees who can access the stored videos.

Tom's Takeaway: As the world becomes more connected, it is imperative that you step back as a consumer and make informed decisions regarding the technology you utilize and your expectations of privacy. While technology has its advantages, at times the security and privacy implications will often exceed the benefits. As a consumer, you need to be aware and prepared to make that determination. One of our hopes with our monthly *Cyber Roundup* is that we continue to increase your awareness and empower you to make informed and balanced decisions.

- **Microsoft was identified as having mistakenly exposed 250 million customer records.** The records date as far back as 14 years ago. Security researchers had identified a set of servers improperly secured that granted anyone access to the customer service and support logs. The logs detailed conversations between the support agents and the Microsoft customers and included such information as e-mail address, support ticket number and the nature of the call. The issue was immediately fixed upon notification to Microsoft.

- **Texas-based Manor Independent School District fell victim to a phishing e-mail that resulted in the fraudulent wire transfer of $2.3 million.** The transfer was performed in three separate transactions over the course of November and December. Initial investigations identified that multiple people had been targeted with the phishing e-mails; however, only one responded and performed the transfers. Full details regarding the incident have not yet been disclosed.

Tom's Takeaway: With all the fancy security solutions that companies persistently market, it is often easy to forget that while technology does have a role, a large part of solving the cyber challenge is the education and awareness of the users. For cybersecurity to be effective, it needs to account for **People**, **Process** and **Technology**, in that order. In this circumstance, if the School District had implemented the correct controls around the awareness of the people and the process of wire transfer, I am very confident in saying this could have been prevented. If you need assistance in developing and ensuring a security posture across your people, process, and technology, please feel free to contact me.

- **U.S. troops being deployed to the Middle East have been instructed to leave at home their personal electronic devices (e.g.,laptops, mobile phones, tablets, etc.).** The concern is that the usage of these devices may expose military operations and place the soldiers in danger, specifically through the use of social media and such inadvertent acts as the devices connecting to the cellular towers in the foreign country allowing the tracking of troop movements.

- **Ransomware continues to be one of the prominent cyber threats.** As the months go by and we continue to publish our *Cyber Roundup*, one thing is certain: the risk of ransomware is not only increasing, but the tactics used are evolving. The silver lining is that you do not have to become a victim. If you need assistance and want to reduce the likelihood of becoming another statistic, please feel free to contact us . Below are the ransomware events for January:

    - On January 8th, the City of Las Vegas alerted of a ransomware event that impacted systems and caused service outages. The City responded quickly to the incident and was able to resume full operations within 12 hours.

    - Telemarketing firm, The Heritage Company, was forced to shut down operations as it looks to restructure after experiencing significant losses stemming from a ransomware attack back in October. The Company ultimately paid the ransom; however, it was unable to recover all services months later, costing the Company a substantial amount of money.

    - A new variant of ransomware, called the Maze ransomware, has been identified as not only encrypting the data on the systems but now also stealing a copy of the data and threatening to publish the data should the ransom not be paid. A listing of companies has already been published by the ransomware gang as refusing to pay. The City of Pensacola and Southwire Cable, both victims of the Maze ransomware, have had gigabytes of files published. The listing of companies on the website continues to grow, some of which have not yet gone public of the breach.

- Richmond Community Schools, a Michigan school district, was forced to extend the winter recess as a result of a ransomware attack that impacted their key systems. The attack is believed to have occurred by way of a network connection with the heating and ventilation service provider. It is not believed that any student data was compromised.

Tom's Takeaway: This breach on the Michigan school district is all too reminiscent of the Target breach back in 2013 that was also the result of the connected HVAC vendor. It is very common when we perform our assessment that we find client networks unknowingly over-exposed to third parties. Understanding and managing your third party risk is key. If you need assistance, please contact us.

- **Hackers targeted and compromised the social media accounts of 15 National Football League teams**. The attack is being attributed to a Saudi hacking gang, dubbed OurMine. The attackers compromised and defaced the Twitter, Facebook, and/or Instragram accounts of the teams.

- **The stolen payment details for 30 million Wawa customers has surfaced for sale in the dark web.** In December 2019, Wawa reported that it suffered a breach of its point of sale systems that resulted in the theft of payment card data. The cards have been made available for sale in the dark web market place called Joker Stash. The average price of the number for sale is $17.

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, twelve offices in New York, New Jersey, Connecticut, Maryland and Rhode Island, and more than 800 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 2020, 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.

Our Firm provides the information in this e-newsletter for general guidance only, and it does not constitute the provision of legal advice, tax advice, accounting services, or professional consulting of any kind.