Cyber Roundup – March 2021

By Thomas J. DeMayo, Principal, Cybersecurity and Privacy Advisory

As we recognize the one-year anniversary of the COVID-19 lockdown in the tri-state area and look forward to light at the end of the tunnel, we should acknowledge the huge part that technology plays in our lives. We can only imagine life without Zoom, or online banking, or streaming services. Working from home would be near impossible, so would schooling our children or internet grocery shopping. Thus, all the more important to keep our personal and business devices and platforms free from potential harm and cyber secured.

Key Cyber Events

The following is a rundown of what happened during the month of February 2021. We welcome your comments, insights and questions.

- **As part of February's *Identity Theft Awareness Week*, the Federal Trade Commission (FTC) released a report noting the following metrics related to 2020:**

  - The biggest increase in identity theft was related to unemployment fraud. In 2019, the FTC received 12,900 claims. In 2020, the FTC received 394,280 claims − a 2956% increase.
  - Identity theft to receive government-sponsored small business loans approximately doubled, going from 43,290 in 2019 to 99,650 in 2020 − a 130% increase.
  - Tax identity theft to receive stimulus payments ended with 83,290 in 2020, up from 27,450 in 2019 − a 203% increase.

  Tom's Takeaway: As demonstrated in the statistics, the pandemic created the perfect environment to prey on the identities of individuals. As we move further into 2021, we are again noticing an increase of identity theft specifically related to unemployment fraud. Unfortunately, no individual should assume their identity is private and protected without taking additional measures. Some of the key steps you and your family should be taking are as follows:

  1. Monitor your accounts and credit reports.
  2. Lock your credit with each of the three credit bureaus. For more information, visit the below websites:
     - https://www.experian.com/freeze/center.html
     - https://www.transunion.com/credit-freeze
     - https://www.equifax.com/personal/credit-report-services/
  3. Establish a PIN with the IRS to secure the filing of your tax returns:
     - https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin

- **A Florida water treatment plant suffered a breach in which the threat actor attempted to increase the amount of lye in the system to more than 100 times normal levels.** Fortunately, system operators noticed the increase and corrected the levels before any risk to the public was sustained. The threat actor is believed to have obtained access to a remote access tool installed on one of the systems used to manage the operations.

- **Global cybercrime costs reached $1 trillion in 2020, according to a report by Atlas VPN.** $945 billion of those costs was due to cybersecurity incidents, and $145 billion related to the cost of placing increased security restrictions.

- **According to RiskRecon, only 8% of the companies impacted by the notorious SolarWinds breach applied the security update to fix the vulnerability.** The companies it identified as still running the vulnerable instances were across all sectors.

  Tom's Takeaway: This report is alarming and signifies just how far behind many businesses continue to be in developing a reasonable cybersecurity program. It has become an unfortunate reality that many have become numb to all the reported breaches and to some extent accept it. We need to remember that this battle impacts each and every one of us. While breaches can and will occur, we need to hold the companies accountable that act in negligence and ultimately cause harm to individuals. Not applying a patch to a highly publicized breach is negligence. This is where senior management and the Board need to ensure they are having the necessary discussions internally and are creating accountability for the cybersecurity programs for which they are ultimately responsible. If you need assistance in knowing and managing your cyber risk, we are here to help.

- **The social video sharing app Tik Tok agreed to pay $92 million in settlement of a class action lawsuit filed in Illinois that claimed the app failed to obtain consent to collect biometric data by way of facial and fingerprint scanning.** Unique to Illinois law is that it allows a private right of action, meaning consumers can directly place a lawsuit with the companies that violate the law.

- **Virginia has become the latest state to enact a comprehensive privacy law, similar to California.** The law is slated to go into effect January 1, 2023. It will impact those doing business in Virginia or directly marketing to Virginia residents. As with the California law, individuals will be given the right to access, correct, delete, know, and opt-out of the sale and processing for targeted advertising purposes of their personal information

- **In a study released by Deep Instinct, it is noted that ransomware increased by 435% in 2020 when compared to 2019.** February 2021 is no different in that upward trend. Below is a summary of the ransomware events that occurred in February:

  - Bombardier, the business jet manufacturer, suffered a breach that resulted in the theft of data from one of their file transfer applications. As part of the ransom, the threat actors began posting the stolen data on their controlled website showing confidential data such as airplane designs and flight test reports. As of this writing, it is not known if the Company has paid the ransom.

  - The California DMV reported a data breach after a third party contractor was hit with ransomware. The contractor, Automatic Funds Transfer Services, was used to verify changes of addresses. The breach may have impacted the prior 20 months of vehicle registration records consisting of name, address, license plate number, and vehicle identification number. The service did not possess any information such as a SSN.

  - Car company Kia Motors suffered a ransomware attack with the threat actors demanding $20 million in payment. The threat actor locked both the car maker's systems and exfiltrated data. The threat actors have given the car maker three weeks to make payment. Should they delay, the ransom may be increased to $30 million.

  - Trucking company Forward Air Corporation experienced a ransomware attack in December. In the 8-K form filed with the SEC, the Company disclosed that the ransomware event cost it $7.5 million in lost revenue and costs to recover from the incident.

  - A new ransomware variant has been identified as now having self-spreading properties. Once in the network, the ransomware will attempt to automatically infect other machines that are connected. One of the most notorious and first self-spreading ransomware variants was WannaCry back in 2017.

- **To end on a lighter note, the Texas Department of Public Safety accidentally sent out an Amber Alert to be on the lookout for the killer doll Chucky.** The description noted that Chucky was a 28-year old doll, 3'1" tall, weighing 16 lbs., and was dressed in blue denim overalls, a multi-colored striped long sleeve shirt, and wielding a huge kitchen knife. The department noted

this was intended to be an internal Amber Alert test; however, it accidentally went live and was sent to the public. *Hidey-ho. Ha-ha-ha.*

Contact Us

Thomas J. DeMayo, Principal, Cybersecurity and Privacy Advisory
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, fourteen offices in New York, New Jersey, Florida, 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 27th on *Accounting Today*'s 2020 "Top 100 Firms" list. It is also ranked among the top 20 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.