KNOW GREATER VALUE™

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Cyber Roundup – March 2018

By Thomas J. DeMayo, Principal, Cyber Risk Management

Welcome again to the month's multifaceted world of cyber criminality. Precipitated by spoofing, spamming, sniffing, sandboxing, phishing, spyware, ransomware, adware, etc., the results are an almost infinite number and variety of cyber crime. All aspects of our individual and business lives are now infused with electronic technology of some sort. It's unavoidable and, actually, should be welcome because it empowers us. BUT knowing the vulnerabilities for ourselves and our businesses is the first step to self-preservation and from there we can go on to use the technology to its utmost benefit.

While there are no absolute "fixes," we invite you to contact Tom DeMayo, Principal, Cyber Risk Management, to explore how we may help you safeguard the security of your organization, business, clients and constituency.

Key Cyber Events

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

- **As tax season heats up, so are the phishing and money scam attempts by cyber criminals.** In a new type of scam, cyber criminals were identified as using stolen personal information to file tax returns and have the refund deposited into the victim's account. Once deposited, the cyber thieves would reach out to the victim and tell them the refund was in error and demand they return the money. To enhance the legitimacy of the claim, the victim was sent a link to a webpage that had all the personal details of the individual, including the transaction, to make it appear as a legitimate case file.

- **The FBI released a public service announcement alerting of W-2 phishing campaigns.** The fraudulent request of W-2 information is a common tactic during tax season. To execute the scam, the cyber criminals will most often impersonate senior executives and e-mail human resource personnel requesting all W-2 information on the employees. The city of Keokuk, Iowa was the most recent victim of this scam, resulting in the disclosure of W-2s of city employees and officials.

- **A phishing attack on a third party vendor of Forrest General Hospital resulted in the exposure of patient protected health information.** The third party vendor, HORNE LLP, provided Medicare reimbursement services. The breach was identified on November 1, 2017 as a result of phishing e-mails being sent from the compromised employee's e-mail. Upon investigation, it was identified that the employee was phished the day prior, resulting in the compromise. Only the one employee account was breached.

- **Tesla's cloud environment was breached and used to mine cryptocurrency.** The cyber criminals were able to gain access to a console used to manage applications and, as luck would have it, the console also contained credentials to Tesla's Amazon Web Service, which was subsequently used to mine the cryptocurrencies. Tesla noted that the compromise did not result in the exposure of any customer data. Over the past months — as cryptocurrencies have exploded — attackers have been diligently identifying ways to exploit any device they can to mine them. In February, it was disclosed that hackers hijacked millions of Android devices to mine Monero coins.

- **A number of interesting cyber security statistics were disclosed in February.**

    - In a report published by McAfee, it is estimated that cybercrime costs businesses $600 billion. That is approximately a 35% increase from 2014's estimated cost of $445 billion. 2017 was a record year for the number of identified security vulnerabilities increasing 31% from 2016, with a total of 20,832 published security flaws.
    - According to Visa, credit card counterfeit fraud in the U.S. dropped 70% between December 2015 and September 2017. This is directly related to the adoption of EMV chip cards. However, the adoption of EMV chip technology has resulted in "card not present" fraud, such as online sales, to become the favored approach for credit card fraud.
    - According to research by advisor firm Javelin Strategy and Research, a record 16.7 million Americans were victims of identity theft in 2017, with losses estimated to be $16.8 billion.

- **Chase.com suffered a computer glitch that resulted in Chase customers logging into their bank accounts and being presented with another customer's details.** The incident happened on February 21 and resulted in the exposure of other customer details, including checking, saving, and credit card account information. Chase acknowledged the incident and confirmed it was not the result of a computer hack, but an internal error.

- **Equifax informed the Senate Banking Committee that the 2017 breach included more data than what was originally disclosed.** Equifax added to the list of personal information stolen to include tax identification numbers, e-mail addresses, and phone numbers. While the material damage has already been done, these additional identifiers just further assist the cyber criminals in using the information to commit identity theft or further target the victims.

- **Ransomware attacks targeted the Colorado Department of Transportation and the cities of Allentown, Pennsylvania and Savannah, Georgia.** The Colorado DOT was infected with ransomware on February 20 and resulted in the shutdown of 2,000 computers. The Colorado DOT has noted it will not pay the ransom and will restore its systems. Allentown and Savannah were both infected on February 13. Allentown is estimating the cost of the attack to be approximately $1 million. While each entity was affected differently, they all impacted government operations and service areas. The specifics on how the ransomware attack was launched has not been disclosed, but it is believed it was likely the result of a phishing attack.

- **An Austrian security firm, SEC Consult, discovered critical vulnerabilities in Mi-Cam baby monitors that could allow hackers to take over the device and spy on children.** It is estimated that 50,000 baby monitors produced by the company have these vulnerabilities. The company has been alerted multiple times since December 2017; however, they have yet to respond. As products continue to be released by companies that have internet connectivity, always challenge the security of the product and don't just assume it is safe. Do your homework on what the product is and what track record the vendor has in creating secure devices. First and foremost, ask yourself the question, "Do I really need to access this device remotely?"

Contact Us

Thomas J. DeMayo, Principal, Cyber Risk Management
CISSP, CISA, CIPP/US CPT CEH CHFI MCSE

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 28th on *Accounting Today's* 2017 "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 2017, 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