KNOW GREATER VALUE™

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Cyber Roundup – February 2018

By Thomas J. DeMayo, Principal, Cyber Risk Management

Back in the 1980s, in addition to fire and flood precautions, safeguarding company equipment and documents came down to a "key" to a door and/or to a file cabinet and maybe a "combination" to a safe or a vault. These days, the pervasiveness of technology-driven security cameras provides additional protection for us and our property. If we back-up our electronic documents offsite, should a fire or flood (or other natural disaster) occur today, data loss can be greatly mitigated — thus leaving us with our major challenge: ***restricting access to our electronic data by outsiders***. So, when you are reviewing your safety and security needs, be sure to call on us to help you assess your electronic data security and adopt measures to preclude some scheming hacker from compromising your business.

Key Cyber Events

The following is a rundown of what happened during the month of January 2018. We welcome your comments, insights and questions. Please contact Tom DeMayo, Principal, Cyber Risk Management, to explore how we may help you safeguard the security of your organization, business, clients and constituency.

- **Two major vulnerabilities were identified by researchers in Intel processor chips dubbed Meltdown and Spectre.** The vulnerabilities could result in the theft of sensitive information such as passwords, credit card and Social Security numbers. Given the prevalence of Intel chips across the world, the implications of this now and in the future are alarming. While patches have been released, many consumers have reported experiencing system crashes as a result of the patches. We recommend proceeding with caution at this point when installing any of the patches and to make sure you perform thorough testing.

- **Three different healthcare organizations suffered major Ransomware attacks.** Allscripts [a major electronic health record provider], Hancock Health [an Indiana based hospital] and Adams Health Network [another Indiana based hospital] all reported being infected with a variant of Ransomware dubbed SamSam. The SamSam ransomware, unlike most ransomware, does not rely on phishing techniques to infect organizations. Cybercriminals target internet facing systems and, once breached, identify key systems internally to encrypt with the ransomware. Of the three impacted healthcare organizations, Hancock Health is the only known entity to pay the ransom. It is reported that Hancock Health paid $55,000 to regain access to their systems. This is a stark reminder that healthcare entities are prime targets for cyberattacks.

- **In a disturbing find, the personal information of babies and infants has been identified for sale on the Dark Web.** The information is currently for sale at a cost of $300 per record on the "Dream Market." It is reported to contain the Social Security numbers, dates of birth and mother's maiden name. The ad on the market is accompanied by the sales pitch "Infant fullz get em befor tax seson." Unlike most personal information, the identity information of children is sold at a premium given their clean credit record and the length of time the fraud can go undetected. It is often not until the children become adults and start to open lines of credit that the fraud is uncovered. Once the criminals obtain the information, it can be used not only for lines of credit, but to file fraudulent tax returns, add a child tax credit to a tax return, or obtain government assistance. While we need to be vigilant in protecting our own personal information, we also need to consider our children regardless of their age.

- **Coincheck, one of Japan's largest cryptocurrency exchanges, suffered the largest known theft of virtual currency as a result of a cyber hack.** It is estimated that the exchange lost approximately $534 million. Coincheck has vowed to make good on the theft and reimburse the 260,000 users affected. While the full details of the attack are not known, the theft is reported to have been isolated to the exchange's "hot wallet," a term used to describe the storage location of the digital assets that are connected to the internet. Coincheck reportedly stored the majority of the assets in the "hot wallet." Best practice for most exchanges is to store the assets in "cold wallets" or locations that are isolated from any external connection to reduce the risk of theft from cyber-based attacks.

- **In 2017, cyber criminals stole $172 billion from 978 million consumers across 20 countries.** This statistic has been provided by Symantec in their 2017 Norton Cyber Security Insights Report. The report makes it clear that the cyber criminals are winning. The report points out that the majority of the attacks are the results of consumers not practicing basic cyber security best practices and still falsely assuming that they will not be a victim. We have expressed in many of our ***Cyber Roundups*** the need to educate people as part of an effective cyber security program. If we cannot get the message across to our readers and help reshape their cyber behaviors, the battle is lost.

- **Maersk, the global shipping company, announced that they are expecting losses of approximately $200-$300 million resulting from significant business disruptions from the August 2017 NotPetya global ransomware attack.** Maersk announced that in the wake of the attack they needed to reinstall 4,000 new servers, 45,000 new workstations, and 2,500 applications. While Maersk suffered a significant loss, it managed to repair itself over the course of ten days. Given the number of servers, workstations and applications reinstalled, such a task would not have been possible if they weren't well-prepared. If you do not currently have a well-designed incident response, disaster recovery and business continuity plan, the survivability of your business can be in jeopardy. If you need help developing a plan, or would like your plan reviewed, we have specialists who can assist in this area.

- **Approximately $1 million has been stolen from U.S. ATMs by hackers.** In a theft dubbed "jackpotting," attackers have been targeting ATDs manufactured by Diebold Nixdorf and modifying them to dispense money as if you won the jackpot. In order to perform the theft, the attackers need physical access to modify the internals of the machine. It is reported that the attackers tend to favor ATMs located in big stores, drive-thrus and pharmacies.

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.