KNOW GREATER VALUE™

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Cyber Roundup – January 2018

By Thomas J. DeMayo, Principal, Cyber Risk Management

Another year behind us as technology marches onward. The pace is breathtaking: remember describing to your grandparents how a fax machine works? Now, try explaining the “cloud” or “wifi” or “cryptocurrency.” With these awesome cyber capabilities comes a need for heightened awareness. Just as brilliant as the minds are that bring us these new technologies, so are the minds of the bad actors working to take advantage of them. If you or your business requires IT consulting and support, please call on PKF O’Connor Davies for help.

Key Cyber Events

The following is a rundown of what happened during the month of December 2017. 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.

- **The Uber hack was attributed to a 20-year old Florida resident living with his parents.** Concealed as a “bug bounty,” Uber paid the hacker $100,000. [Bug bounties are a common technique used by many large organizations looking to identify vulnerabilities before they are exploited by cyber criminals.] The size of the reward is often tied to the severity of the vulnerability. While Uber did have a bug bounty program, the circumstances surrounding the hack and payment are not consistent with how a bug bounty program would typically operate. The former CEO, Travis Kalanic, was aware of the breach; however, it is still unknown who authored the payment to the hacker.

- **A database containing 1.4 billion user names and passwords was identified in a dark web forum.** The treasure trove of credentials appears to be linked to 252 previous breaches. To date, this is one of the largest credential databases discovered, almost double the size of the previous largest exposure of 797 million. Password breaches are going to continue to happen. It is key that users remember to follow best practice password types, such as using long passphrases instead of passwords and ensuring passwords are not the same across websites.

- **A report listing the 100 worst passwords for 2017 was released by the company SplashData, the makers of a password manager.** The five most common passwords in the list were 123456, password, 12345678, qwerty and 12345. This is consistent with the information obtained from the database containing 1.4 billion credentials discussed in the prior bulleted item. Passwords such as abc123, password1, iloveyou and 1q2w3e4r5t were also very popular. We agree that passwords are cumbersome, but they are often our only option. We have found password managers such as LastPass, SplashData, OneLogin, etc. to be very effective in helping consumers manage the burden of passwords in a secure way. If you are not using one, it is worth investigating the potential benefits.

- **Cybercriminals are starting to shift away from Bitcoin in favor of other cryptocurrencies.** Bitcoin prices continue to surge, transaction fees rise and the price stability becomes increasingly volatile. Virtual currencies play a key role in supporting the cyber underground market. The majority of the criminal transactions supported by Bitcoin are low dollar amounts, making the high transaction fees a significant impact on profit margins. Cybercriminals are starting to favor other cryptcurrencies such as ZCash, Etherum, and Monero. While transaction fees play an important role, a key benefit of these other cryptocurrencies is that, unlike Bitcoin, they are designed to offer full anonymity of transactions performed.

- **Alteryx, a marketing and analytics company, suffered a breach that exposed the information of 123 million American households.** What has become a common trend, the data was identified in an unsecured Amazon cloud service storage bucket. While the data did not contain information such as SSNs or account information, it contained other information across 248 categories such as home address, phone number, mortgage ownership, age and personal interests. While the information itself can't cause direct harm — such as opening lines of credit — information like this is invaluable to hackers looking to target individuals with very specific social engineering campaigns.

- **A cybercriminal group shifted their Ransomware tactics by allowing the victims to set their own price**. The Ransomware variant, Scarab, was designed under the concept that victims will be more likely to pay if they have more control over the price. It is believed this tactic is also being deployed to offset the volatility of Bitcoin pricing and gives the cybercriminals greater control.

- **Yapian, the owners of the South Korean cryptocurrency exchange, Youbit, has filed for bankruptcy in the wake of a hack that resulted in the loss of 17% of its cryptocurrency.** Until the bankruptcy process is complete, the company is only allowing customers to withdraw 75% of their assets. While cryptocurrencies have the opportunity for tremendous financial gains, this is a reminder that they also have tremendous financial risk.

- **A New Jersey teen has been charged with hacking into the systems of a Bergen County high school to change his grades.** The teen allegedly hacked into the school's Genesis student management system as well as the Naviance system, a nationwide system used by colleges to retrieve transcripts of applicants. Once the student changed the grades, he immediately submitted his applications to the Ivy League schools he was hoping to attend. The hack was identified when a guidance counselor noticed the changes. Over the past few months, schools have been consistently in the headlines as a result of cyber related incidents. Any school —public or private — should strongly consider evaluating their cybersecurity program against not only the external threats, but the threats posed by internal resources looking to gain a competitive advantage.

- **Two major software flaws were identified in Microsoft and Apple products.** Microsoft identified a major vulnerability in their Malware Protection Engine that would allow an attacker to remotely execute code and allow for complete control of the system. Microsoft released an out-of-band patch to address the vulnerability corresponding to CVE-2017-11937**.** If you have not done so, make sure your systems are patched. A major software vulnerability was also identified in Apple iPhones running iOS 11.1.2. The exploit would allow a hacker to gain access to the underlying operating system. Apple has also released an update to address the vulnerability.

- **In a poll conducted by CyberArk, 50% of IT security decision-makers claimed that their firms did not fully disclose the details of data breach.** Such a statistic is fairly alarming coming on the heals of major consumer data breaches such as Equifax. [***Editor's observation:*** We consider the biggest fundamental problem is that the majority of organizations — big and small — have not fully embraced the seriousness of the cybersecurity threat and continue to regard cybersecurity as a business expense as opposed to a business necessity and enabler. Herbert Spencer, an English philosopher and sociologist, once said "the great aim of education is not knowledge but action." We all have been educated on how serious the cyber threat is; now, we just need to take action to defend against it.]

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