KNOW GREATER VALUE™

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Cyber Roundup – December 2017

By Thomas J. DeMayo, Principal, Cyber Risk Management

The cyber news for November runs the gamut: from shopping scams to hackers-for-hire; from schools being targeted to cryptocurrency security bugs. While efforts are being made by the best and the brightest among us to ensure the protection of our data and its use, we still have to face the possibility that we will become victims — as they say "it's not if, it's when." Call on PKF O'Connor Davies for a cyber "check-up," for preventative measures that may be implemented now, and for help should a breach occur in the future.

Key Cyber Events

The following is a rundown of what happened during the month of November. 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 Better Business Bureau released a scam alert warning holiday shoppers.** A scam has been identified which attempts to lure shoppers to fake websites offering amazing deals on various products. The website will allow the shoppers to complete the purchase and will also provide a tracking number; however, the products will never be delivered. As the holiday season continues, so will the efforts of cyber criminals to take advantage of shoppers. The key tip is to remain vigilant and remember: ***if it seems to be too good to be true, it probably is.*** **P**ause, **I**nspect and **T**hink ("PIT") before visiting any unfamiliar website or completing any online purchase.

- **ISIS was identified hacking school websites across the U.S**. Approximately 800 U.S. school websites were hacked and resulted in the posting of a YouTube video. The video contained images of Saddam Hussein with text displayed stating "I love Islamic State (ISIS)." An audible Arabic message was also contained in the video stating "There is no God but God. Muhammad is the prophet of God." The websites were all managed by a common vendor, SchoolDesk. The vendor is fully cooperating with the FBI in the investigation. This is the second month in a row that U.S. schools have made the headlines as a result of being targeted by hackers. As hackers have now set their sights on schools, it is important for all public and private schools to assess their current cyber security program to ensure they have reasonable defenses.

- **The FBI has charged a 22-year-old with installing keyloggers on the University of Iowa's systems to facilitate the manipulation of grades and receiving advance copies of exams.** Over a period of 21 months, from March 2015 to December 2016, the student allegedly installed keyloggers on university computers in class rooms and labs. Once the keyloggers were installed, the student had access to any data that was typed on the machine by the professors, inclusive of credentials to the university's student management and e-mail system. It is believed the student used the stolen credentials to change his/her grades approximately 90 times over the 21-month period.

- **Apple disclosed a major security flaw of their most recent operating system, High Sierra, that would allow any user with access to the machine to gain full administrative access.** This could be abused by either a person with local access or malware that is installed on the machine. Apple was quick to acknowledge the flaw and issue a fix. If you have not already done so and you are running any Mac with High Sierra, make sure you apply the patch as soon as possible.

- **Uber, under new leadership, announced that they suffered a breach affecting 600,000 drivers and 57 million users in 2016.** While that sounds bad enough, they also disclosed that they paid the hackers a $100,000 ransom not to disclose the breach and to delete the stolen data. Failure to disclose a breach is in direct violation of numerous state privacy laws. While the full consequences of Uber's actions are yet to be known, Uber has further established themselves as the poster child of a corporation having poor governance and a broken culture of compliance.

- **2017 has broken the record for software-based security vulnerabilities, according to a study by Risk Based Security.** Not including the quarter ended December 2017, there were 16,006 vulnerabilities disclosed through September 30, 2017. For all of 2016, 15,832 vulnerabilities had been disclosed — a record-setting year at that time. As more of the world continues to become automated and software is increasingly intertwined with our day-to-day lives, it will be a natural progression for the number of vulnerabilities to continue to increase. What will be crucial is the vulnerability identification and management process implemented by your organization to manage the ever-growing risk.

- **300 million in cryptocurrency has been potentially lost as a result of a software bug in a crypto wallet.** The crypto wallet vendor, Parity, is in the process of fixing one vulnerability that resulted in the theft of $32 million by a hacker. The vendor mistakenly allowed a single user to take ownership of all existing multi-signature wallets. (A multi-signature wallet is designed to promote greater security by requiring multiple users to enter their key before funds can be transferred.) When the user realized the accidental transfer and tried to fix the issue, it resulted in all of the wallets becoming inaccessible with no way for anyone to retrieve the funds. Parity is continuing to work on a resolution. Cryptocurrency is still in its infancy. Any user of cryptocurrency needs to fully understand that it is not only extremely volatile in value, but also has many underlying security and operational issues that need to be addressed.

- **The Australian Broadcasting Corporation (ABC) and the U.S. Army Intelligence and Security Command (INSCOM) are the latest entities to report a breach as a result of incorrectly configured Amazon Web Service S3 storage buckets.** The ABC incident resulted in the disclosure of thousands of email addresses, logins and password hashes. The INSCOM incident resulted in the exposure of files classified as Top Secret and various forms of stored authentication data. Reporting on this type of misconfiguration has become a monthly occurrence. As more and more organizations are embracing the cloud, they are doing so without fully understanding the ramifications and risks associated with the potential openness of the cloud. If you are considering the cloud or have already moved to the cloud, make sure your risk management program has been updated to manage the unique risks it creates.

- **U.S. Federal prosecutors in Minnesota have charged a man for hiring three hacking services to launch a year-long denial-of-service campaign against his former employer**. A denial of service attack is designed to flood a company with an enormous amount of internet traffic so that their servers can no longer process legitimate data. While the termination of an employee has always

had an element of risk, as the commoditization of hacking services continues to evolve, it is likely we will see more hacker-for-hire services targeting former employers.

- **New York Attorney General Eric Schneiderman announced his proposal of a new data security bill called the SHIELD Act (Stop Hacks and Improve Electronic Data Security Act).** The bill is designed to ensure that any business that holds sensitive data of New York residents has implemented reasonable administrative, technical and physical safeguards to protect the data. Violations of the law would permit the Attorney General to bring suit and civil penalties. Given the significance of some of the recent data breaches, it is likely we will see proposed legislation like this across the U.S.

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.