KNOW GREATER VALUE™

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Cyber Roundup – December 2018

By Thomas J. DeMayo, Principal, Cyber Risk Management

Is your organization ready for a review of its current cybersecurity policies and procedures? How about a "phishing" test? Do your employees need cyber awareness training? How are your cyber controls over electronic fund transfers? What about monitoring the controls of any third party that provides your business with cyber services?

Think about these questions as you peruse the latest issue of our *Cyber Roundup*. Resolve that 2019 is the year you are going to make solid attempts to secure your business against cyber sabotage. **Ring in the new cyber safeguards, ring out the old cyber vulnerabilities.**

Key Cyber Events

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

- **Marriott announced a massive breach affecting 500 million guests who made reservations at their Starwood properties around the globe.** What may become one of the most massive breaches to date, it is being estimated that of the 500 million guests affected, approximately 327 million had a combination of highly sensitive information stolen such as a passport number, address, phone number, date of birth, arrival and departure dates, etc. Credit card numbers and expiration dates were also compromised although Marriott cannot yet confirm if the cyber criminals were able to decrypt the information. What is most concerning is that the breach went undetected for four years.

  Marriot has set up a website for people to obtain more information at the following address: https://answers.kroll.com/. It is currently offering a free membership to WebWatcher to help monitor a guest's personal information for abuse. Further, if guests believe they have experienced fraud as a result of their passport being breached, Marriot will pay for the replacement. While it is too soon to identify how much the breach will end up costing Marriot, estimates go as high as $1 billion. With the new GDPR regulation in effect, fines could go as high as 4% of the worldwide annual revenue. If you have been impacted by this breach, it will be important to change your account passwords, monitor your credit card statements and also any loyalty accounts that you have with Marriott.

- **Private messages from approximately 81,000 Facebook users were identified for sale.** The information was selling for around ten cents per account. The information was stolen through a malicious web browser extension that allowed the hackers to monitor and obtain the private communications. Two months prior, in October 2018, hacker forums were listing Facebook credentials for sale costing between $3 and $12. Given how significant Facebook is as a company and the massive amount of information they hold on individuals, as well as the impact they have, it only stands to reason that attacks against Facebook will continue in frequency and sophistication over time.

- **An Indiana school district, Lake Ridge Schools, lost $120,000 in a fraudulent wire transfer.** The e-mail account of the Business Manager was accessed by a cyber criminal. With access to the account, the hacker e-mailed a request to the District's banking institution, BNY Mellon, and requested the transfer of funds to various individuals listed as contractors. The bank complied with the request. The District brought a lawsuit to reclaim the funds; however, the lawsuit was dismissed and the U.S. District Court judge determined the bank was not responsible for the loss under their contracts. It is not entirely uncommon for banks not to return funds in the event of a

fraud like this. While many will do so in good faith, they could easily claim they are not responsible when transfers are the result of potentially poor cyber security controls of the customer. The cyber risk management of a business is one of the key areas that should be assessed and understood.

- **East Ohio Regional Hospital and Ohio Valley Medical Center were the latest victims of a Ransomware attack.** The attack resulted in the emergency room being unable to take patients and redirecting ambulances to nearby hospitals. Fortunately, procedures were in place to account for system failures and the staff quickly resorted back to paper charting. It is not believed that any patient data was compromised during the attack.

- **Kars4Kids and Make-A-Wish Foundation are two of the latest not-for-profits to suffer cyber incidents.** This goes to demonstrate that if a business is for-profit or not-for-profit, cyber criminals will not discriminate. NFPs are often favorite targets of cyber criminals, knowing they often don't have the resources to build effective cybersecurity programs.

    - Kars4Kids suffered a data breach as a result of an unsecured database exposed to the internet. Approximately 21,000 records were impacted consisting of personal information on donors, their e-mail addresses, tax receipts and other credentials.

    - The Make-A-Wish Foundation had their website targeted to launch a cryptojacking attack against visitors to the website. Visitors to their website would execute a program that would result in the visitor's machine mining cryptocurrency on the cybercriminal's behalf. It is believed the site has been infected since May 2018. The website was made vulnerable as a result of an unpatched update to the website's content management system, Drupal.

- **Atrium Health, a North and South Carolina healthcare system, announced a breach impacting 2.65 million patients.** The breach was not directly the result of Atrium Health but, rather, a third party billing company, AccuDoc Solutions. AccuDoc notified Atrium that an unauthorized third party had obtained access to AccuDoc's database between September 22-29, 2018. The information impacted included: name, address, dates of service, medical record number, invoice number, balance, insurance information and social security numbers. As with any third party, a new level of risk is introduced. While third parties are often key to a business's operations, it is critical that strong due diligence and monitoring controls exist to ensure that the third party you select has the security controls necessary to protect the data you are entrusting them with. If you need assistance performing third party information security and/or privacy due diligence for any of your vendors, please feel free to contact me.

- **Through a SIM swapping account, $1 million in cryptocurrency was stolen from a San Francisco-based investor's CoinBase crypto wallet.** SIM swapping is an attack whereby the cybercriminal contacts a mobile provider's customer service and asks them to assign a number to a new device. Once the cybercriminals have control of the number, they can obtain access to necessary authentication codes sent to the phone and gain access to targeted accounts.

- **HSBC alerted the public to a security incident that impacted an undisclosed number of individuals.** The attack occurred between October 4-14, 2018. The incident is believed to be the result of a credential stuffing attack whereby usernames and passwords stolen or obtained from other incidents are used. The type of information impacted included: names, addresses, phone numbers, account numbers, account types, balances, statement history, etc. HSBC initiated procedures for customers to change their passwords and has offered to provide credit monitoring and identity theft protection for impacted customers.

- **A study performed by SailPoint indicates that high risk employee security behaviors continue to persist and are getting worse.** From the 1600 global employees surveyed, the following metrics were obtained:

    - 75% of respondents reuse passwords across personal and professional accounts. Up from 56% in 2014.
    - 23% only change their passwords two times or fewer per year.
    - More than half the respondents view the IT department as an inconvenience while 13% would not immediately inform IT if they were hacked.
    - 31% installed software without informing or obtaining approval from IT.

What is concerning is the number of individuals reusing passwords. While this may sound benign, it isn't. Since the same password is reused across websites, the increased exposure of the password increases the likelihood of it being breached. Cyber criminals know all too well that employees like to reuse passwords and will leverage the breach of one site to target other accounts used by the employee. Such tactics were used in the HSBC breach listed above. To help businesses manage this threat, PKFOD recently launched a Dark Web Monitoring service that will allow companies visibility into how exposed they may be on the dark web and what credentials are for sale of their employee accounts**. If you would like us to perform a sample search for your company domain name, please contact me directly.**

Contact Us

Thomas J. DeMayo, Principal, Cyber Risk Management
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, 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 29th on *Accounting Today's* 2018 "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 2018, 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.