KNOW GREATER VALUE™

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Cyber Roundup – October 2018

By Thomas J. DeMayo, Principal, Cyber Risk Management

As we say often, the objective of our *Cyber Roundup* is to inform our readers of what's going on in the cyberworld — much like reading alerts about various health threats posted by medical news sites. They keep you "in the know." Should you think you are experiencing symptoms, you would likely schedule an appointment with the appropriate health professional. You may also schedule periodic medical exams for preventative reasons.

Think of us as your "cyber doctor." We can perform a "check-up" of your system(s), conduct tests, make recommendations and referrals, and generally assist you in managing the well-being of your IT infrastructure. Don't procrastinate. The doctor is in.

Key Cyber Events

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

- **Effective September 21, 2018, the act of enabling a Credit Freeze on an individual's Credit File is now free and extends to minors under the age of 16 years.** A Credit Freeze is the act of locking your credit file and blocking any lender from checking your file. If a lender cannot check your file, the lender — in most cases — won't issue a line of credit in your name. Prior to the new law taking effect, certain states could charge a fee for the act of locking and unlocking a credit file. In addition, when it came to minors, certain states allowed credit freezes to be placed and others did not. Cyber criminals particularly like to target minors with identity theft because it often goes undetected for an extended period of time.

  In the wake of the Equifax breach, one of the key protections promoted to consumers was to place a credit freeze on their file. When many realized this was a fee-based protection, outcry ensued. If you have not done so, it is highly recommended that you place a credit freeze on all your credit files and any minors in your care. To do so, you can visit the following websites:

  - TransUnion
  - Equifax
  - Experian

- **California passes a first-of-its-kind Internet of Things cybersecurity law**. The bill, SB-327, was signed into law by the Governor of California, Jerry Brown. Effective January 1, 2020, any manufacturer of a device that will have the ability to connect to the internet must be designed to have reasonable security features. One of the key requirements is that if the device can be accessed remotely with a password, every device must have a unique password. This addresses a key flaw that cyber criminals have leveraged over the past few years to take control of millions of devices with the same password and create massive botnets.

- **Bristol Airport, located in South West England, was impacted by a Ransomware attack.** Fortunately, the attack had limited impact and only resulted in the flight information screens being taken off line. In this situation, the airport was able to respond quickly and prevent the

spread of the malware before any critical systems were impacted. Further, they had contingency plans in place to account for the flight information screens being offline. This incident serves as a prime example that incidents can and will occur. The question is: are you ready to respond with well-designed contingency plans to maintain operations? To further enforce the point that preparation is key, in a separate and unrelated event, a Denver printing company was forced to close and is claiming a recent ransomware attack is to blame because the company was unable to recover after the incident.

- **Facebook made the headlines in September as a result of the following two incidents:**

    - **Facebook admitted to using the phone numbers its members supplied for two-factor authentication for ad targeting.** Two-factor authentication was implemented and encouraged by Facebook to ensure a greater degree of security around user accounts. What wasn't clear was the fact that a push for greater security may lead to a decrease in privacy.

    - **Facebook suffered its largest security breach to date, affecting approximately 50 million users.** The vulnerability identified would have allowed the cyber criminals the ability to login as the affected users and access their information. The vulnerability has since been fixed; however, the full details of the incident have not yet been disclosed.

- **The Consumer Information Notification Act (H.R. 6743) was passed by the House Financial Services Committee with the objective of standardizing the data security and breach notification process for financial institutions.** The bill, if ultimately passed, will amend the long standing Gramm-Leach-Bliley Act (GLBA). Currently, breach notification is state-specific and dependent. If the bill is passed, the new law would preempt state data breach laws and require all financial institutions to notify consumers of a data breach.

- **The Government Payment Services website, GovPayNow.com, exposed personal information on approximately 14 million people.** The website and service is used across many U.S. state and local governments to accept online payments. The vulnerability allowed users to access copies of receipts of other individuals. The information leaked consisted of: names, addresses, phone numbers and the last four digits of their credit card.

- **The SEC fined Voya Financial Advisors, Inc., a broker-dealer based in Des Moines, IA, for cybersecurity program failures that resulted in the compromise of customers' personal information.** As a registered broker-dealer, Voya is required to maintain compliance with the Identity Theft and Red Flags rules, which require them to protect consumer personal information from the risk of identity theft.

- **For the first time, a cyber insurance policy is being offered to individuals.** Insurance provider Saga recently announced it will include personal cybercrime coverage in its insurance policies. The coverage will protect those insured against risk from their personal devices.

- **Google was identified to have paid Mastercard millions to gain access to the offline transactions of users.** The agreement — which is being reported as a "secret" agreement between the two companies — was designed to allow Google to analyze the data to determine if ads resulted in sales at physical stores. This was in support of a new tool Google is developing called Store Sales Measurement to allow businesses to track the conversion of online ads to retail sales.

- **A relatively new Russian hacking forum has been identified selling access to 3,000 breached websites.** The website, name MagBO, essentially sells the buyer a way of accessing the website to take control. Prices range from $1 to $1,000. While such hacking forums are common, this

does serve as a reminder that any business with a website needs to ensure it is securely programmed and managed.

- **A flaw was identified in a Freedom of Information Act (FOIA) request portal that exposed sensitive personal information such as SSNs and immigrant identification numbers.** FOIA was put into law to allow any U.S. citizen the right to obtain access to government information. The FOIA portal was designed with the intention of centralizing, streamlining and better safeguarding the requests to any of the 116 agencies subject to FOIA. The flaw has since been fixed; however, it is believed to have occurred due to a design error during a system upgrade process.

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.