Cyber Roundup – October 2017

By Thomas J. DeMayo, Principal, Cyber Risk Management

Gone are the days when we heard the word "fishing" and looked forward to a day on the lake, when a "hack" was another name for a trick or shortcut that increases productivity and efficiency, or when the "web" referred to a spider's handicraft in our basement. So, let's see what happened last month in the cyberworld. In so doing, we will see the scope of criminal behavior conducted with simple computer tools. We will also see how companies are stepping up with exposing the criminal behavior, mitigating its damage and guarding against its recurrence. Lessons learned.

Key Cyber Events

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

- **Whole Foods Markets experienced a breach of customer credit card information.** Certain venues, such as taprooms and table service restaurants in select stores, were affected. The breach did not affect regular grocery shoppers. Details on which locations were targeted have not been released. An investigation is ongoing with the assistance of law enforcement and an outside cybersecurity firm.

- **Deloitte, a leading global tax and auditing firm, announced that it suffered a breach of confidential information, including e-mails and private documents of their clients.** The attack, discovered in March, is believed to have first occurred in October or November of 2016. The attack targeted an administrator account that granted the hackers access to Deloitte's e-mail system. The investigation is ongoing and a full disclosure of the clients impacted has not been released.

- **Webroot's *Quarterly Threat Trends* reports 1.4 million new phishing sites are launched each month.** This is about a 30% increase since its report released in December 2016. [Phishing sites are websites created and controlled by the attackers to steal sensitive information.] In order to prevent becoming a victim of phishing, employees need to know how to identify phishing tactics. This dramatic increase demonstrates now — more than ever —that employee security awareness training needs to be a key component of any security program.

- **TigerSwan, a U.S. military contractor, was alerted in July to an unsecured Amazon S3 storage container with the resumes of individuals seeking employment with the contractor.** The resumes included candidate personal information, such as social security, passport and driver license numbers. TigerSwan had contracted with a third-party recruitment service provider, TalentPen, that was responsible for the setup and management of the S3 bucket as part of the recruitment service. This breach demonstrates that third-party risk is only going to continue to increase as more businesses use third party services to manage their data. Strong vendor due diligence and monitoring cannot be neglected.

- **The SEC disclosed that the EDGAR platform containing the financial details of publicly-traded companies was breached.** Stephanie Avakian, co-director of the SEC's Enforcement Division, stated "Cyber-related threats and misconduct are among the greatest risks facing investors and the securities industry."

- **The SEC established a new Cyber Unit dedicated to investigating cyber-related offenses — such as market manipulation schemes and illegal blockchain based activities — in relation to finance laws.** Stephanie Avakian, co-director of the SEC's Enforcement Division, stated "Cyber-related threats and misconduct are among the greatest risks facing investors and the securities industry."

- **In connection with three massive data breaches at Yahoo between 2013 and 2016, a U.S. District Court Judge has cleared the way for a class action lawsuit seeking compensation for damages.** Those breaches disclosed the personal information of over 3 billion users. Verizon, who acquired Yahoo in June, faces potential monetary liability that could well exceed the $4.8 billion it paid to acquire Yahoo. This demonstrates the importance of adequate IT and cyber risk considerations for any merger or acquisition activities.

- **The NotPetya ransomware attack in June is estimated to have cost FedEx $300 million according to its latest earnings report.** The attack, which significantly disrupted operations, ultimately resulted in FedEx being unable recover all of its systems impacted by the ransomware. Ransomware threats are not going away and, as we see with FedEx, can have a major financial impact. Ensure that your incident response strategy has accounted for Ransomware events.

- **According to statistics released by Kaspersky Lab, approximately 1.65 million machines have been infected with malware that turns the machines into cryptocurrency miners on behalf of the cyber criminals.** This is a dramatic increase from prior years. Cryptocurrency mining is the process by which computers are used to perform mathematical computations to create new cryptocurrency funds. In exchange for the mining efforts, the funds are returned to the miners. Cryptocurrency mining is legal; however, using the machines of other individuals without their permission is not.

- **September saw an increase in the use of hacked LinkedIn accounts to send phishing links in direct private messages.** The phishing efforts were designed to steal login credentials. This demonstrates that just as with e-mails, we need to be aware and cautious with any links or attachments we receive from any communication channels. Pause, Inspect and Think (PIT) before taking any actions.

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 440 locations, in 150 countries around the world.