KNOW GREATER VALUE™

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

# Cyber Roundup – May 2018

By Thomas J. DeMayo, Principal, Cyber Risk Management

Before we get to this month's cyber events — which many of you may consider to be "jaw-dropping" in their intensity and reach — let's be reminded of the FBI's list of steps that should be taken to help protect your computer from intrusion:

- Keep Your Firewall Turned On
- Install or Update Your Antivirus Software
- Install or Update Your Antispyware Technology
- Keep Your Operating System Up to Date
- Be Careful What You Download
- Turn Off Your Computer When Not in Use

Contact Tom DeMayo if he and his staff can be of assistance to you as you ensure the safety of your digital operations.

## Key Cyber Events

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

- **1.5 billion business and consumer files where identified unsecured across the internet by security researchers of the threat intelligence firm, Digital Shadows.** The documents included a wide range of data, inclusive of sensitive data such as tax returns, payroll information, medical records, credit cards and intellectual property. The exposure was the result of a number of different services being misconfigured, such as Amazon S3 buckets, FTP sites, and exposed network attached storage devices.

- **The risk of "typosquatting" domains was brought to light by investigative reporter Brian Krebs and security expert Matthew Chambers when they uncovered unsecured access logs of over 1000 dot-cm domains.** Typosquatting is a technique used by hackers to purchase very similar domain names associated with popular sites that the hackers believe the users may land on as a result of mistyping. In this situation, the attackers targeted individuals that would mistype sites ending in COM with CM by missing the "O" key. Once individuals land on these sites, they may be infected with malware or the likes. The sites, which included many name brands, e.g., (itunes.cm), (aol.cm) and (espn.cm), were identified as being visited approximately 12 million times in 2018 so far. To prevent making this mistake, consider bookmarking the sites you frequently visit.

- **Saks and Lord & Taylor reported a breach of approximately 5 million credit and debit cards.** The hacking group, Fin7, offered the cards for sale on the "Jokers Stash" credit card marketplace located on the dark web. It is believed the majority of the information came from the New York and New Jersey locations.

- **The social network app, Grindr, was identified as sharing the HIV status of its users with third parties.** Grindr was sending the data to two analytic companies, Apptimize and Localytics. In addition to the HIV status, it also included items such as GPS location, phone number, e-mail address, etc. Apptimize and Localytics are services used by the company to monitor and analyze how the app was being used. Grindr has since stopped sharing that type of information with third parties. While the legitimacy and necessity of the transfer can be debated in either direction, in the wake of the Facebook—Cambrdige Analytica situation, this is just another reminder to be cautious of the sites you use and the information you share.

- **Mobile security firm, Lookout, reports that mobile phishing attacks are up 85% annually.** The report notes that 66% of e-mails are first opened on a mobile device and that users are three times more likely to click on a suspicious link on a phone than on a workstation. The report highlights that the traditional phishing protections are not adequate for mobile devices. From the small screen, truncated URLs, links in traditional text messages and the multitude of other apps that can be used to send links, a new approach needs to be devised.

- **Security researchers identified a flaw in Amazon's Alexa that could allow a malicious developer to trick Alexa into recording everything a person says.** It is not known if any hackers have successfully exploited the flaw. Amazon has since implemented a fix for the issue. This is the 2nd issue made public where researchers identified that Alexa could be manipulated to eavesdrop. Maybe instead of saying "Hello" Alexa, we should be saying "Goodbye" Alexa.

- **Panera Bread's website, Panerabread.com, was identified as leaking millions of customer records.** The information appeared to belong to any customer who registered for an account to order food online. Such information as name, e-mail, address, birth date and the last four digits of the credit card number where exposed. A security researcher identified the issue and notified Panera back in August 2017; however, the company did not address the issue until it was reported to and investigated by, the cyber security journalist Brian Krebs.

- **A new hacking group dubbed, Orangeworm, has been identified by Symantec as targeting the healthcare sector.** The group, unknown until now, can be linked to hacking activities identified back in 2015. The group does not appear to operate randomly but is very selective in the victims they target. Once a target company has been selected, the hacking group will attempt to gain a foothold in the environment and install a backdoor granting it access. Once inside, they will look to move and infect other machines. While a motive is not known, it is believed that the attacks were in support of corporate espionage.

- **In the wake of the ransomware attack against Atlanta, it is reported that the city spent $2.6 million on emergency efforts to respond.** The attackers were originally asking for approximately $55,000 in Bitcoin to unlock the systems and data encrypted by the ransomware. As with most cyber incidents, the bulk of the expenses related to incident response and digital forensics. Of the $2.6 million, $600,000 was paid to the firm facilitating the incident response.

## 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.

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.