KNOW
GREATER
VALUE™

PKF
O'CONNOR
DAVIES
ACCOUNTANTS AND ADVISORS

Cyber Roundup – August 2017

By Thomas J. DeMayo, Principal, Cyber Risk Management

Last month was "business as usual" for cyber criminals. Even so, the volume and extent of these activities are mind-blowing — particularly with respect to the targeting of children, how easy cyber hacking skills can be transferred and cloud security. As computer professionals become aware of each incident, solutions eventually follow. In the meantime, we stay alert and pay attention to IT recommendations.

Key Cyber Events

The following is a rundown of what happened during the month of July. 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 FBI issued a public service announcement alerting parents and guardians of children to the dangers and privacy concerns of internet connected toys ("Smart Toys").** The announcement states: *These toys typically contain sensors, microphones, cameras, data storage components, and other multimedia capabilities — including speech recognition and GPS options. These features could put the privacy and safety of children at risk due to the large amount of personal information that may be unwittingly disclosed.* If you have or care for children, this article is well worth the read.

- **Six billion records have been exposed in the first half of 2017 as a result of data breaches, according to a report issued by Risk Based Security.** This number already exceeds the record 4.2 billion records exposed for all of 2016. The United States accounted for 61% of the breaches.

- **Kaspersky, once considered a premiere anti-virus vendor, has been removed from the U.S. government's approved vendors list.** Over the past few months, concerns have surfaced that the anti-virus vendor's software may be manipulated on behalf of the Russian government to allow access to secure U.S. government systems.

- **Two new Cybercrime-as-a-Service offerings were identified targeting individuals with minimal computer skills aspiring to become "hackers."** The services are designed to easily distribute malware to steal passwords from internet browsers or to create phishing campaigns to trick people into providing their credentials. Interestingly, not only are these services easy to operate for beginning hackers, they are also extremely low cost — less than $15.

- **FedEx, in the wake of the NotPetya ransomware that circled the globe in June, stated that it may not be able to recover all of the affected systems.** The financial impact is likely to be material. FedEx did not have cyber insurance to help recover some of the financial losses. Once the smoke settles, it will be interesting to see what the actual dollar amount lost is.

- **Ethereum, a form of cryptocurrency, was the victim of four cyber attacks during the month.** Hackers successfully seized approximately $40 million in the cryptocurrency by targeting various software vulnerabilities and using traditional phishing techniques. As cryptocurrencies continue to gain traction, it is inevitable that attackers will go on looking for ways to exploit the cryptocurrency ecosystem.

- **Verizon and Dow Jones each released announcements that customer records had been exposed as a result of incorrectly-secured Amazon cloud storage services.** Verizon announced that 14 million records were left exposed, containing personal information, such as names, cell phone numbers, and account PINs that can be used to access the account. Dow Jones reported 2.2 million customer records were left exposed containing details, such as names, home and e-mail addresses, account details and the last four digits of credit card numbers. These issues bring to light that the cloud is not a security panacea. While the cloud does provide some great advantages, for it to be secure, it needs to be configured correctly.

- **A serious vulnerability — dubbed Devil's Ivy — that could allow attackers to fully take over thousands of internet-connected devices ranging from security cameras to access card readers was disclosed by a security firm**. While a patch has been released, given the sheer number and how widespread these devices are located, it is unlikely the problem will go away any time soon. While companies continue to ramp up the production of internet-connected devices, issues like this are only going to become worse unless there is a fundamental shift in the security approach these companies take.

- **Apple users were alerted to two dangerous malware strains targeting the Mac platform.** The first strain — dubbed OSX Dok — is an existing malware that has now been enhanced to mirror websites of major banks in an effort to steal Mac users' banking credentials. The second strain of malware — dubbed FruitFly — is a newly-discovered piece of malware that is believed to have been in existence, but remained undetected, for the past 10 years. FruitFly allows the attackers to take control of webcams, screens, mice and keyboards and to install additional software to further compromise the devices.

- **The Hard Rock and Loews hotels are the latest hotel chains to announce that the credit card numbers and personal information of customers may have been stolen as a result of cyber criminals infiltrating the third-party booking system used by the chains.** The incident relates to the Sabre Corp's breach announced back in May. Sabre provides a software-as-a-service reservations system that is used by many travel agencies, hotels and booking services, such as the Hard Rock and Loews hotels.

- **The Ashley Madison parent company reached an $11.2 million settlement agreement in relation to the 2015 data breach that exposed the personal information of their subscribers.** Ashley Madison is an adult dating website designed to facilitate extramarital affairs. As a result of the settlement, six million users may be eligible for compensation.

- **Vulnerabilities identified in the Tesla Model X allowed security researchers to remotely control the car's brakes and doors**. The attack targeted the car's built-in and internet-connected web browser. Tesla was notified of the issue and immediately issued a fix.

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.

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