KNOW GREATER VALUE™

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Cyber Roundup – September 2018

By Thomas J. DeMayo, Principal, Cyber Risk Management

Although cyber criminality continues, it is clear that it is being monitored actively, forces are being marshaled against it, and — for the most part — computer users are not lulled into a false sense of security. That is why we prepare our *Cyber Roundup* each month – to ensure that our readers stay aware of the breadth and depth of cyber crime. It also speaks to the transparency that must occur when a company becomes aware of a cyber event that must be reported to the authorities and to the public, as well as the "fix" that must be developed and available to victims as appropriate.

PKF O'Connor Davies combines in-depth accounting, auditing and tax knowledge with its forensic, analytical and litigation skills. Into that environment, our IT team's background in new and emerging technologies is leveraged, enabling us to spot threats and trends, investigate the full range of devices that store digital data, and resolve incidents related to possible cyber crime.

Better to be data-savvy, than data-stolen.

Key Cyber Events

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

- **Two federal cyber actions took place in August:**
    - **President Trump signed a presidential order revoking guidelines established by former President Obama that placed various restrictions on the use of offensive cyber operations.** The new presidential order is intended to allow the U.S. to respond faster and more aggressively to cyber attacks using cyber offensive strategies.
    - **President Trump also signed into law the NIST Small Business Cybersecurity Act.** The law will require the National Institute for Standards and Technology (NIST) to provide cybersecurity guidelines, tools and best practices for small to medium size businesses.
- **A number of interesting statistics by the security research community were presented in August that are worth noting, including:**
    - **Valimail research determined that approximately 6.4 billion fake emails are sent each day.** Based on the metrics they used, the actual number is probably quite larger; however, this is a good indication of the extent of the problem.
    - **A study by RiskIQ calculated that $1 million is lost every minute to cybercrime.** In addition, it identified that within that minute 1.5 organizations are victimized by ransomware with an average cost of $15,221.
    - **In the first half of 2018, 2.6 billion personal data records have been breached.** While the number is still astronomical, it is 3.4 billion less than the 6 billion records breached in the first half of 2018.

- **Two separate incidents resulted in the exposure of customer security account PIN numbers for T-Mobile and AT&T.** Such numbers are used by the providers to authenticate that the customer is the owner of the account.

    - **In the first incident, an Apple online store security oversight resulted in the exposure of approximately 77 million T-Mobile customer account PINs.** This was the result of a coding error that allowed an attacker to try an infinite number of customer PIN combinations until the correct one is identified. Such an attack is known as a ***brute force attack***. Typically, programmers should include application logic to stop processing the requests after a low threshold of failed successive attempts is reached. For example, after the fifth failed attempt, the application will lock the account and require the provider to be contacted to proceed.

    - **In a separate and unrelated incident, customer PIN numbers of AT&T subscribers who purchased phone insurance through Asurion were also potentially exposed.** This was again the result of a programming error that allowed an individual to gain access to the PIN code if they knew the phone number. It is not known how many AT&T customers may have been exposed by this breach.

- **The FBI was active in issuing cybersecurity warnings and identifying new cyber threats.** The warnings and events are as follows:

    - **The FBI alerted the public to the rise of cyber extortion scams.** These scams are designed to specifically use stolen personal information of the victims to entice the victims to pay. Last month we reported on a variation of this scam regarding sextortion, in which stolen credentials of individuals that existed on the dark web were used to trick victims into believing their computers had been hacked and are under the control of the cybercriminal.

    - **The FBI issued warnings to the banks that a sophisticated and global fraud scheme was identified that would target the banks with an ATM cash out attack.** Such an attack is when the cybercriminals use cloned cards to withdraw funds from ATM machines. This alert was the result of a breach of an unidentified card issuer and intelligence that the cybercriminals were planning to use it in a choreographed global attack. An Indian bank appears to be the only victim of the cash out, suffering a total loss of $13.5 million ($11.5 million in ATM cash outs and $2 million in fraudulent fund transfers).

    - **The FBI identified North Korean malware — dubbed KEYMARBLE — that is used to attack U.S. government entities and perform such actions as stealing sensitive data and capturing screenshots or keystrokes.** Such tools are known in the cyber security community as Remote Access Trojans (RATs). The malware is operated under a group called HIDDEN COBRA, which has a notorious reputation of being highly sophisticated.

- **Google is being sued for a privacy violation of tracking user locations even if they explicitly opt to not be tracked by turning off their location history.** Google has since updated their privacy policy to clarify that even with location history disabled, the location data will be stored by other Google services such as Search or Maps. As we have seen with various new privacy laws such as the General Data Protection Regulation (GDPR), privacy notices and practices need to be clear and transparent. The basis for this lawsuit is that Google was not clear with its practices and the process of disabling tracking is not intuitive for a regular user. As time goes on and the privacy

consciousness of individuals continues to increase, such lawsuits like this will become commonplace.

- **A significant bug was identified with new Apple MacBooks that would allow an attacker to compromise the device immediately upon first boot and connection to WiFi.** The bug takes advantage of apples Device Enrollment Program (DEP). DEP is designed to streamline the deployment of new apple devices by automating the configuration and enrollment of the devices with a company's mobile device management solution. Apple has since fixed the bug. This serves as a reminder that the notion that Apple devices are inherently more secure is not accurate and Apple users need to be vigilant with basic security controls such as consistent patching and anti-virus.

- **UnityPoint Health alerted of a breach affecting 1.4 million patient records**. UnityPoint Health is a multi-hospital group operating in Iowa, Illinois and Wisconsin. This is the second major breach it has disclosed this year. We reported on the first breach back in April 2018 when it identified multiple employee e-mail accounts that contained patient information were hacked resulting in the exposure of information on 16,400 patients. In the most recent attack, UnityPoint was the victim of a business e-mail compromise attack. In this particular attack, the cybercriminals impersonated a senior executive, tricking the employees into responding and disclosing their e-mail credentials. We continue to stress that employee training is key in order to defend against these types of attacks. Over the years, we have developed very effective and engaging training programs to specifically address these types of attacks.

- **Adams County in Wisconsin reported a breach affecting 258,000 citizens.** The breach is believed to have lasted and gone undetected for around six years. The County has reported that suspects have been identified; however, they have not yet been disclosed. The breach is believed to be the result of a malicious insider and not an external cyber criminal. In a statement released by the county, they indicate that unauthorized individuals obtained additional access rights and user names and passwords by manipulating county software that allowed them further access to other systems to which they were not authorized. In our experience, the majority of the smaller municipalities, such as counties and towns, have not yet embraced a holistic cybersecurity program to defend against internal and external cyber threats. Often, this is the result of capital expenditures for cybersecurity not being considered or approved.

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.