KNOW GREATER VALUE™

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Cyber Roundup – March 2019

By Thomas J. DeMayo, Principal, Cyber Risk Management

In a perfect world, we would not have to concern ourselves that our IT infrastructure and devices are not self-secured and impervious. Unfortunately, even the latest equipment and programs can eventually succumb to infiltration by bad actors. We also have a need – whether of necessity or by choice – to go faster and get more from our personal and business technology.

Because our reliance on IT is growing, cybersecurity must take center stage. If the last bulleted item below doesn't illustrate the need for speed, nothing will. Now's the time to take proactive, safeguarding measures. Obviously, everyone can't be a technological wizard, so let PKF O'Connor Davies be your expert of choice.

Key Cyber Events

The following is a rundown of what happened during the month of February 2019. We welcome your comments, insights and questions.

- **A third-party e-mail provider, VFEmail, suffered a hack that destroyed all e-mails stored by the company going to back to 2001.** Unlike many hacks that will demand a ransom, this hack was designed to destroy all the systems, inclusive of the backup systems. While the systems were eventually brought back online, the data has not yet been recovered. This incident serves as a reminder that third-party risk cannot be underestimated. As companies increasingly use third-party providers, an effective due diligence process is key. If you need assistance with your due diligence program, please feel free to contact us.

- **According to a report released by Bromium, Inc., *Social Media Platforms and the Cybercrime Economy,* cybercriminals are earning $3.25 billion by leveraging social media.** The report exposes how social media is used to perform malicious activities, such as distribute malware by way of malicious links and ads, and sell illicit goods and services, such as drugs or hacking tools. This serves as a reminder that no different than an e-mail, social media is a risk that can't be ignored. From malware infections to data loss, organizations and employees need to be educated on the risk of social media.

- **Cybercriminals were identified offering lucrative salaries to skilled hackers.** Posts on the dark web revealed that the cybercriminal organizations will offer upwards of $1 million per year for experienced hackers. This was identified in a post offering $64,000 per month year one and up to $90,000 per month year two. Another post was trying to find an individual to help extort high-worth individuals for a starting pay of $30,000 per month.

- **2.7 million recorded phone calls containing medical information were found exposed to the internet.** The recorded calls belonged to a Swedish-based healthcare website known as 1177.

- **Payroll software provider, Apex Human Capital Management, suffered a ransomware attack.** While the company claims customer data was not impacted, operations were shutdown. The company paid the ransom to restore operations as soon as possible. Although the attackers provided the necessary decryption keys, the process did not fully work as promised rendering many files useless, delaying restoration. As companies plan out their incident response, business continuity and disaster recovery plans, ransomware needs to be factored into the equation and restoration strategies defined and tested to ensure operations resume in an entity-approved timeframe.

- **TikTok, a video sharing app, agreed to a record $5.7 million settlement for violating the Children's Online Privacy Protection Act (COPPA).** COPPA is a federal law designed to protect the privacy of children under 13 years of age by requiring any website or online service directed toward children to obtain parental consent before collecting and processing the child's information. The FTC's complaint alleges that TikTok knew children were using the app but failed to obtain parental consent.

- **Turbo Tax was the target of a credential stuffing attack resulting in compromised tax returns and the highly sensitive information they contain.** Credential stuffing is when attackers leverage user names and passwords from other breaches knowing users often use the same password or slight variations across multiple websites. In this situation, TurboTax was not a victim of a breach, but instead, the impacted users were the victims of poor password management practices.

- **The Energy & Commerce Committee's Subcommittee on Consumer Protection and Commerce, a key House subcommittee, began exploring a new federal privacy bill.** The hearing acknowledged that a federal law is warranted; however, the debate is on how prescriptive it should be. As the world becomes increasingly digital, privacy is an issue that will not go away. If not addressed at the federal level, it is almost certain that the states will start to pass their own privacy legislation.

- **The Dow Jones exposed a watchlist of 2.4 million high-risk individuals and corporate entities.** The exposure was the result of an incorrectly secured Amazon Web Service database. Companies can subscribe to and use the list in the course of operating their risk and compliance program. A spokesperson for the Dow Jones disclosed the issue was the result of an undisclosed third party. The issue has since been corrected.

- **CrowdStrike, a cybersecurity firm, leveraged their incident investigation data to shed some light on how long it takes nation-state hackers and generic cybercriminals to move laterally in an environment once breached.** In other words, after the hackers infect just one machine, how long does it take them to start breaching other machines and moving further into the environment. The breakdown is as follows:

    - Russia – 19 minutes
    - North Korea – 2 hours and 20 minutes
    - China – 4 hours
    - Iran – 5 hours

    The report further identified that regular cybercriminals are the slowest of the group, coming in at 9 hours and 42 minutes.

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