Cyber Roundup – January 2019

By Thomas J. DeMayo, Principal, Cyber Risk Management

Concerning this month's *Cyber Roundup*, a Millennial might text **SSDD** [the "polite" translation being: **same stuff, different day**]. Just another typical month in the annals of cyber security. We have hacked emails, breached websites, phishing schemes and the potential of privacy incursion. And then there's children's credentials for sale on the Dark Web, weak passwords and lack of cyber defenses. Welcome to 2019.

Call us if you want help in averting cyber damage to your business.

Key Cyber Events

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

- **Australia passed a first-of-its-kind law that will allow law enforcement agencies to require tech companies, such as Facebook, Google, etc., to help decrypt messages used in suspected terrorism or crime.** Across the globe, law enforcement agencies have been struggling with not being able to access encrypted electronic communications. While the law certainly fills a law enforcement need, privacy and security implications could arise. How this law is implemented will need to be watched closely to ensure that proper checks and balances exist to prevent abuse. Further, it will be critical to ensure that whatever mechanisms are built into these platforms to allow access to these "backdoors" will be engineered appropriately to mitigate the risk of the backdoor falling into the wrong hands.

- **The San Diego Unified School District alerted of an identified hack that resulted in the breach of approximately 500,000 personal records.** The breach resulted in the exposure of personal data of students and employees going back almost 10 years to 2008. The information included items such as name, date of birth, Social Security number, address, and health information. The attack, which lasted over a period of 11 months, is believed to be the result of targeted phishing e-mails designed to steal the employees' credentials. Fifty employee accounts are believed to have been breached by way of the phishing emails. This serves as a reminder that employee cyber awareness education and phishing training is essential. One of the best areas any company can allocate their cyber defense budget is on education. All too often, companies take a check box approach to this requirement and require employees to simply watch a video once a year. For cybersecurity awareness to be effective, it needs to be ongoing and built into the culture of the company.

- **The Chinese government made the headlines as a result of the following events:**

    - The Chinese government breached a diplomatic communications network used by the 28 European Union members to communicate on policymaking details. The hack appears to have been the result of a phishing attack.

    - The Marriott hack that resulted in the breach of 500 million Starwood Hotels customer data, reported in last month's *Cyber Roundup,* has been linked to a Chinese government spy agency. While a definitive statement has not yet been made, the tools, tactics and procedures used are consistent with the Chinese agency.

- **The Equifax breach reported in September 2017 that resulted in the unauthorized disclosure of highly sensitive information of approximately 143 million consumers has been declared as being preventable by the U.S. House of Representatives Committee on Oversight and Government Reform.** The report — found here — discusses many of the security pitfalls of the company. What is key to the report is that the Committee ultimately concluded that "Equifax failed to fully appreciate and mitigate its cybersecurity risks. Had the company taken action to address its observable security issues prior to this cyberattack, the data breach could have been prevented." This is a very powerful statement that our readers should reflect on personally and professionally. We encourage every business leader to have an honest discussion with your management team and your board about how well your cyber risks are understood and managed. If you have not had a detailed or effective cybersecurity study, it is never too late and we are always here to help.

- **NASA reported a cyber breach impacting employees' personal data.** The breach, consisting of highly sensitive data, such as Social Security numbers, impacted employees onboarded, offboarded, or transferred during July 2006 to October 2018. The investigation is ongoing. What is concerning is that the Office of Inspector General has noted information security issues of the agency in numerous reports over the years; however, NASA has not been timely in addressing the issues noted.

- **A repository of 40,000 credentials belonging to government portals around the world has been identified by a Russian cyber security firm.** The credentials are believed to have been harvested by malware operators of the infected machines. As with any stolen credentials, it is only a matter of time — if it has not occurred already — that these credentials will make their way for sale in hacking forums in the Dark Web.

- **1-800-Flowers Canadian website suffered a breach that resulted in the credit card information of its customers being stolen over a four-year period.** The breach is believed to have occurred between August 15, 2014 and September 15, 2018. The main 1-800-Flowers website was not impacted. The number of impacted customers has not yet been disclosed.

- **A new stock of personal information of children has been identified for sale on the Dark Web.** It is reported to contain the Social Security number, date of birth, address, etc. of these children. One of the ads claims to have obtained the information from pediatrician and other medical databases. The ad is further accompanied by the sales pitch "Very cheap and very fresh" and "The kids records obtained come from good families that can provide and pay for medical support." Unlike most personal information, the identity information of children is sold at a premium given their clean credit record and the length of time the fraud can go undetected. It is often not until the children become adults and start to open lines of credit that the fraud is uncovered. Once the criminals obtain the information, it can be used not only for lines of credit, but to file fraudulent tax returns, add a child tax credit to a tax return or obtain government assistance. While we all need to be vigilant in protecting our own personal information, this is a wake-up call that we need to also consider our children regardless of their age and take proactive measures to protect their identity.

- **With the close of 2018, Slashdata, a password security company, released their Top 100 worst passwords for 2018.** The data is collected by analyzing leaked credentials over the year. The study shows that people continue to use weak passwords. The top 10 most common passwords are as follows: 123456, password, 123456789, 12345678, 12345, 111111, 1234567, sunshine, qwerty, iloveyou.

- **A study released by Upstream believes that cyber attacks will cost the automobile industry up to $24 billion over the next five years.** The study, which can be found here, explores the risk of the auto industry embracing connectivity, from autonomous vehicles to ride sharing services. It explores how attacks may come from every angle. The stakes are high for the auto industry, with ramifications resulting in life safety, identity theft and privacy issues. While this report focuses on the auto industry, this problem will impact every industry as more Smart devices are deployed. As society learns to live in an increasingly connected and "Smart" world, part of that education will be to challenge the security and privacy practices of any device we choose to implement or use that is "Smart."

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, ten 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.