Cyber Roundup – April 2019

By Thomas J. DeMayo, Principal, Cyber Risk Management

The weaponization ─ and subsequent monetization ─ of electronic data is clearly on display in this our second anniversary edition of *Cyber Roundup*. The right data can be hijacked for ransom, can be used to target the location of family members, and can be manipulated to alter medical implant devices to name just a few malevolent uses. Although there is much risk in this the digital age, there is also much reward for businesses and individuals alike. We really have no viable choice but to rely on electronic data and devices; however, we cannot fail to be computer savvy and vigilant. Let the Cyber Risk Management team at PKF O'Connor Davies partner with you and your staff to help minimize potential danger.

Key Cyber Events

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

- Ransomware hit with a vengeance in March. The following entities suffered and/or disclosed a ransomware-related event.

  - **Wolverine Security Group (WSG), a Michigan-based medical billing company, began alerting affected individuals of a ransomware attack that impacted their operations in September 2018.** The files impacted 600,000 individuals and included highly sensitive information such as social security numbers, insurance details, etc. WSG was able to conclude that no data was exfiltrated; however, given the type of data affected, breach notifications will be issued and identity protection services offered. The Office for Civil Rights (OCR), the enforcement arm of the Health Insurance Portability and Accountability Act (HIPAA), has made it clear that ransomware, in most cases, is to be considered a breach.

  - **The town of Plymouth, Connecticut suffered a ransomware attack that originated from a malicious e-mail.** The ransomware resulted in municipal and police servers being taken offline.

  - **The city of Albany, New York suffered a ransomware attack on March 30.** As of this writing, not many details have been released; however, the ransomware did impact many of the city's online systems, inclusive of the payroll system.

  - **Jackson County, Georgia paid $400,000 to cyber criminals in an attempt to restore operations after a ransomware attack crippled most of the government's IT systems.** The county did not have a viable backup in place to restore operations, resulting in the only option available ─ pay the ransom. Upon payment, the cyber criminals did provide the key to decrypt the systems.

  - **Norsk Hydro, one of the world's largest aluminum production companies, was forced to shut down operations in the U.S. and Europe as a result of a ransomware attack.** The attack, noted by the company as being "severe," resulted in the switchover to manual operations where possible. The company opted not to pay the ransom, but rather to restore their systems using alternative methods. In a similar event, two U.S.- based chemical companies, Hexion and Momentive, were infected with the same type of ransomware as Norsk, also disrupting operations.

- **Boston's Committee for Public Counsel spent multiple weeks trying to recover from a ransomware attack.** The systems impacted contained cases on clients and the billing system. The Committee did not pay the ransom, but elected to restore the systems from backup.

Tom's Takeaway: Every company, big and small, for-profit and not-for-profit, can and will be targeted by cyber criminals. The key question is, are you prepared? If you need assistance in answering that question, we are only an e-mail or a phone call away.

- **Verifications.io, an e-mail address verifier for third parties, exposed approximately 2 billion consumer records**. The information contained e-mail address, gender, name, IP address, phone number, mortgage amounts, credit scores, interest rates and other personal information. The breach was the result of an improperly secured MongoDB database. Further, none of the data in the database was encrypted, allowing all of the data to be easily read.

- **Three private universities learned of a breach to their admissions system after prospective students received e-mails offering them the opportunity to buy their admission file.** The files contained sensitive information such as comments and decisions. The impacted universities are Oberlin College, Grinnell College and Hamilton College. The details of how the breach occurred have not yet been disclosed. In an unrelated incident against universities, a report by Accenture claims that Chinese hackers have been targeting select U.S. universities to steal military research.

- **The U.S. Homeland Security Department issued an alert with regard to implantable defibrillators produced by Medtronic**. The alert impacts 16 different models across approximately 750,000 devices created by Medtronic. The vulnerabilities identified would allow a sophisticated attacker the ability to alter the programming of the device harming the patient or read sensitive data stored in the device.

- **Facebook users learned that the phone number they provided to better secure their accounts with multi-factor authentication was being used by the social network to target ads and to suggest new connections.** While this is misleading for many reasons, it is just another privacy concern that Facebook will have to address as the world becomes more aware and sensitive to how personal data is used. In a separate incident, Facebook disclosed that an internal review identified that they were storing Facebook and Instagram passwords in clear text. Further, the passwords where searchable by 20,000 internal employees. While an exact number of users impacted is not known, it is believed to be between 200 and 600 million. Facebook intends to alert the impacted users but not force a reset. Facebook has noted that it has found no indication that the data was abused by internal employees.

- **A study released by Barracuda networks revealed the 12 most common subject lines used in phishing e-mails.** The subject lines are as follows: (1) *Request*, (2) *Follow up*, (3) *Urgent/Important*, (4) *Are you available?/Are you at your desk?* (5) *Payment Status*, (6) *Hello*, (7) *Purchase*, (8) *Invoice Due*, (9) *Re:* (10) *Direct Deposit*, (11) *Expenses*, and (12) *Payroll*.

  Tom's Takeaway: When we do employee awareness training, we always emphasize that phishing e-mails are designed to hook into your emotions. Curiosity is one of the most powerful and compelling emotions we have. These subject lines are an affirmation of that fact.

- **Family Locator, an app designed to allow families to track each other's location, was storing the location data in an unprotected database exposed to the internet.** The discovery was made by a security researcher. The database contained information on approximately 238,000 users such as the user's name, e-mail address, clear text password and a record of the family members' locations. None of the data was encrypted and anyone who could find the database could read all of the data inclusive of the users' passwords.

Tom's Takeaway: As the explosion of apps and smart devices continue, issues like this will only become more frequent for the foreseeable future. While an app like this can prove valuable for various reasons, consumers have to balance the risk-reward relationship.

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, eleven offices in New York, New Jersey, Connecticut, Maryland and Rhode Island, 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.