Cyber Roundup – September 2019

By Thomas J. DeMayo, Principal, Cyber Risk Management

All businesses must periodically test their policies and procedures to be proactive in ensuring that they are comprehensive and fit any changing circumstances. Your information technology (hardware, software, archives, programs, staff, etc.) is one such area that must be considered. In this month's issue of *Cyber Roundup*, the incidents of cyber intrusion and mishap serve to support the need for such action. Call us. We can help you test your IT functions and develop an actionable plan to avert potential harm to your business.

Key Cyber Events

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

- **2019 is on course to be another recording breaking year for data breaches**. In a report issued by Risk Based Security, it was stated that 3,813 breaches were reported through June 30, 2019 exposing 4.1 billion records. Compared to the same period in 2018, the number of breaches and exposed records has increased approximately 50 percent.

- **Cabarrus County, North Carolina reported that it fell victim to a business email compromise scam that resulted in the loss of approximately $1.7 million**. The cyber criminals impersonated a contractor engaged by the County to build a new school and requested that the banking information be updated. The County wired $2.5 million; however, the bank was able to freeze some of it once officials realized they were being scammed.

Tom's Takeaway: In April – based on a FBI study – we reported that business email compromise schemes have almost doubled year-over-year for the past few years, reaching 1.2 billion in 2018. If you haven't done so, it is critical that you make sure you have a strong set of controls around the receipt and updating of any banking information from a vendor.

- School districts and municipalities were a hot target for cybercriminals in August. The following key events occurred:

  - **Houston County School District in Alabama had to delay the start of the school year as a result of a malware attack that shut down the District's computer and telecommunications network.** The District did not formally indicate if a ransom was demanded.

  - **Rockville Centre School District on Long Island, New York suffered a ransomware attack and paid approximately $100,000 to regain access to their systems.** The District had cyber insurance that assisted with the payment. The Mineola School District, located nearby, was also infected with the same ransomware but was able to avoid making a payment by restoring their systems from backup.

  - **Twenty-two Texas municipalities were hit with a targeted and coordinated ransomware attack.** The majority of the entities impacted were smaller local governments. The hackers demanded $2.5 million to unlock the systems. It is believed that the cybercriminals leveraged the IT managed service provider of the municipalities to launch the ransomware. The Governor of Texas declared it the second highest level alert in the state's emergency response system.

- **Two companies that provide online services to dental offices around the country, Percsoft and Digital Dental Record, suffered a ransomware attack.** The attack resulted in approximately 400 dental offices being unable to operate. The offices had no access to charts, x-rays, schedules or billing. It is believed the companies paid the ransom to regain access to the systems.

Tom's Takeaway: As a firm, we have a strong history in supporting numerous municipalities in the tristate area. While we understand the budgetary constraints, it is critical that all municipalities begin to view the implementation of a cybersecurity program as a key component of public safety. If your municipality does not know where to start, we encourage you to contact us to learn about how we can assist.

On a separate note, the Texas and dental office incidents underscore how important it is to perform third party due diligence on any IT managed service provider (MSP) or Cloud service you use. Over the past six months, it is clear that the cybercriminals are starting to focus on IT MSPs and Cloud service providers. It is critical that you have a complete understanding of what security controls are in place at those providers. If you need assistance in this area, we would be happy to help.

- **A treasure trove of biometric data was found publicly exposed on the internet by security researchers.** The biometric data consisted of fingerprint and facial recognition data. In addition, data such as unencrypted usernames and passwords, logs, and staff details were also found exposed. The data was identified as belonging to Suprema, a company specializing in biometrics, security, and identity solutions. This is the first known breach of biometric data. The company is investigating the incident.

Tom's Takeaway: While biometrics can perform secure authentication and ease the burden of end users needing to remember passwords, no different than a Social Security number, providers need to exercise extreme care in how they collect and protect this data. Unlike a password, a biometric cannot be changed.

- **The FBI issued a warning regarding dating site fraud.** According to the FBI, they noted a 70 percent increase in confidence/romance scams. In these scams, the fraudsters use dating websites to trick people into various money scams, be it sending money, purchasing gifts, or money laundering. In 2018, the FBI noted 18,000 incidents with losses totaling $362 million.

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 2019 "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 2019, 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.