# Cyber Roundup – January 2020

By Thomas J. DeMayo, Principal, Cyber Risk Management

The decade ended the way it began – with cybercrime in the headlines. As we ease into the 2020s, however, more ways to combat it and more laws to protect us against it are being devised. In the meantime, we need to keep aware and be proactive. Hopefully, reading our monthly *Cyber Roundup* will keep you attentive and responsive to digital wrongdoing and potential protective workarounds.

## Key Cyber Events

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

- **New Jersey's largest hospital system, Meridian Health, suffered a ransomware attack.** The attack, which occurred on December 2, impacted the computer systems of the Hospital and resulted in 100 non-emergency surgeries and appointments to be rescheduled. Meridian Health ultimately paid the undisclosed ransom amount to regain access to their systems.

- **In the wake of a ransomware attack, New Orleans declared a state of emergency.** Phishing attempts and other suspicious activity were identified on December 13. In response to the attack, their IT Department took precautionary measures and instructed all employees to shut down their machines and powered down all servers. Ransomware malware was detected, but no ransom was demanded. The incident is being investigated. A few weeks later, Baton Rouge Community College also suffered a ransomware attack. The college did not pay the ransom.

- **CyrusOne, a major U.S. data center provider, suffered a ransomware attack.** The attack was limited to its managed services business located in one of their New York data centers. Details on how the malware infiltrated the network have not been disclosed.

- **Facebook reported a data breach of employee information.** Facebook announced that a laptop was stolen from a car that contained workers' payroll data, inclusive of banking information, on its 29,000 employees. The laptop was not encrypted. The laptop belonged to a member of the payroll department who was not authorized to remove the laptop from the campus.

***Tom's Takeaway:*** In most modern operating systems, be it Windows or Apple, encryption is a feature that is included at no additional charge. If you are not utilizing encryption on your devices – especially mobile devices – I encourage you to do so. It is a simple and powerful control in protecting your data should your device be lost or stolen.

- **The social media platform TikTok has been banned on government-issued devices by the majority of U.S. military branches.** TikTok is an increasingly popular platform that allows individuals to make and publish short video clips. There is a concern that the Chinese-owned app presents a threat to national security.

- **The German Federal Commissioner for Data Protection and Freedom of Information fined mobile services provider 1&1 Telecommunications with the largest GDPR fine to date, 9.55 million euro.** GDPR, the General Data Privacy Regulation, is an EU regulation that requires the safe handling of personal information. The fine is the result of 1&1 failing to implement proper safeguards over customer records and allowing any caller to access personal information on an account by providing only the name and date of birth.

***Tom's Takeaway:*** GDPR is a comprehensive privacy regulation that applies not only to EU-based companies, but also, in certain circumstances, to U.S. entities that process EU resident data. Should GDPR not apply to your business, this should serve as a reminder that if you maintain records that contain personal information, ensure you have a reasonable process to verify the identity of the caller/requestor before releasing any information. Privacy has become a key issue for many regulatory bodies. If you are not sure if the GDPR regulation applies to your business or would like more information on designing a privacy program, please feel free to contact me.

- **WaWa, an East Coast convenience store chain, reported a massive data breach impacting all 850 locations.** It is believed that the breach started in March and continued through to December. The malware compromised customer payment information, credit and debit card numbers used at any of their in-store payment terminals or fuel pumps. Wawa is providing potentially impacted customers with one year of identity theft protection and monitoring. Additional details on the breach, and what to do if you believe you are impacted, can be found here.

- **TrueDialog, an SMS text message provider, reported a breach that exposed a treasure trove of information.** Security researchers identified an unsecured database hosted in Microsoft Azure, 604 gigabytes in size, containing approximately 1 billion entries. The information exposed consisted of such data as e-mail addresses, usernames, passwords, and text messages. The database was taken offline upon identification.

- **A New York City Hospital IT employee pled guilty to stealing co-workers' data.** Between 2013 and 2018, the perpetrator stole the credentials of his fellow co-workers to obtain access to their e-mail, tax records, social media, and other online accounts. He installed malicious software on the co-workers' machines designed to capture their credentials.

***Tom's Takeaway:*** In the cyber realm, we often forget that attackers exist not only externally, but internally as well. Insiders have a tremendous advantage over external parties as a consequence of the trusted foothold they already have in the work environment. As a business, when you define your cyber/information security strategy, be sure to also account for effectively restricting and monitoring the trusted insider. If you need assistance in performing an insider threat risk assessment, please contact us.

- **Sentara Hospital, located in Norfolk, VA, has reached a $2.2 million HIPAA settlement agreement with the Department of Health and Human Services' Office for Civil Rights (OCR).** The fine was the result of Sentara Hospital failing to report a breach to all impacted individuals when they incorrectly mailed the wrong protected health information (PHI) to 577 patients. Sentara notified only eight of the 577 patients when it incorrectly concluded that for the remainder of the individuals it did not constitute a reportable event. The conclusion was based on the circumstance that the remainder of the letters only included the patient name, account number, and dates of service and not any diagnosis, treatment and other medical information.

***Tom's Takeaway:*** PHI – in the simplest terms – is any information identifiable to a person that is created, used, or disclosed by a HIPAA-covered entity during the course of providing a health care service. When a covered entity (e.g., a hospital) has a breach, the onus is on the covered entity to prove

by way of a documented risk assessment that the information was not disclosed. In the case of Sentara, they clearly misunderstood the breach notification rule and what constitutes a breach. HIPAA compliance is a specialty that requires knowledgeable individuals to navigate the compliance obligations. If you need assistance in understanding your HIPAA compliance obligations, we would be happy to assist.

## 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, twelve offices in New York, New Jersey, Connecticut, Maryland and Rhode Island, and more than 800 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 2020, 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.