Cyber Roundup – November 2019

By Thomas J. DeMayo, Principal, Cyber Risk Management

Although October was designated by the U.S. Department of Homeland Security as **National Cybersecurity Awareness Month**, that didn't stop any of the cybercriminals last month from doing what they do best – key logging, ransoming, hacking, phishing, etc. Just maybe – because you are becoming more and more knowledgeable about the vulnerabilities of the internet – you were able to recognize the possibilities and kept them away from your data using *the best defense is a good offense* approach. Call on us. We can help you.

Key Cyber Events

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

- **The FBI released a public service announcement, alerting that High-Impact Ransomware attacks threaten U.S. Businesses and Organizations.** The alert notifies that ransomware attacks are becoming more "targeted, sophisticated, and costly." The alert discusses the primary methods of ransomware infection – to pay or not to pay and who to notify – and key protections. We encourage you to read the alert.

- **DCH Health System, an Alabama hospital system consisting of three hospitals, suffered a ransomware attack**. The attack resulted in the hospitals having to shift to a manual mode using paper copies. The hospital system paid the ransom – an undisclosed amount – to regain access to the systems.

- **A California medical practice group, Wood Ranch Medical, was forced to permanently shut down after it was unable to recover from a ransomware attack.** The attack resulted in all patient data being encrypted, inclusive of the backups. All medical records stored on the systems have been lost and cannot be recovered. Earlier in the year, Michigan-based Brookside ENT and Hearing Center was also forced to close its practice after a ransomware attack.

- **Florida-based Jackson Health System received a $2.1 million HIPAA violation fine.** The Department of Health and Human Services (HHS) noted that the health system had multiple violations and failed to introduce basic defenses in the safeguarding of electronic protected health information (ePHI). Violations included the lack of a detailed risk analysis, failure to manage risks to acceptable levels, review system and user activity records and restrict access to ePHI. What is unique about this case is that, given the extent of the violations and level of disregard by Jackson Health, HHS imposed a civil monetary penalty rather than attempting to reach a settlement. Typically, HHS will attempt to reach a settlement at a reduced fine that includes the requirements to correct identified deficiencies.

  Tom's Takeaway: Healthcare entities have a tremendous responsibility. Be it socially, morally, and, in today's world, electronically. They have to shoulder the burden of ensuring our health and, equally as important, our privacy. Healthcare entities need to adapt and recognize that in order to provide patient care, they must also develop information and cybersecurity strategies to protect the very sensitive information with which they are entrusted. Cybersecurity needs to be viewed not as a business expense, but as a necessary component of patient care. We work with many healthcare-related entities. If you need assistance, we are only a phone call or e-mail away.

- **IT-managed service providers have proved to be an increasing target during 2019.** In a report released by threat intelligence firm, Armor, thirteen (13) IT-managed service providers confirmed breaches that resulted in ransomware being spread to their customers.

  Tom's Takeaway: In the course of helping clients manage their cyber risk, we interact with many IT-managed service providers. Like any business, some are great, some are OK, and some are concerning. What I often find is that the majority of small to midsize market customers don't perform adequate due diligence on the security of the providers they are trusting to manage their systems and networks. This creates a high-risk blind spot. If you are using an IT-managed service provider, you should have – and they should welcome – an open and transparent conversation about their cybersecurity program and how they have designed their management approach to minimize the risk of their central management to your business. When we perform assessments for clients, this is one of the areas we advise them to allow us to explore on their behalf.

- **The country of Georgia suffered a massive cyberattack that resulted in approximately 2,000 government, news, and court websites being impacted.** Many of the sites were defaced with a picture of the former President Mikheil Saakashvili. The source of the attack is still under investigation.

- **The United States and United Kingdom have joined forces and signed a first-of-its-kind cross-border data access agreement designed to tackle criminals and terrorists online.** The Act, called the CLOUD Act, will allow the U.S. and U.K. law enforcement agencies to request electronic information related to crime, terrorism, child sexual abuse, and cybercrime directly from tech companies based in each other's country. Prior to the Act, the legal process to obtain the information could have taken up to two years.

- **The U.S. Airforce has officially replaced the use of legacy floppy disk drives to manage the country's nuclear arsenal.** Instead of the historic floppy drive, a new secure solid state drive based solution has been implemented. The old system was created in 1968 and ran on an IBM mainframe.

- **A New Jersey man has been arrested for the installation of key loggers on the computers of two rival companies in order to steal trade secrets.** A key logger is a software that is designed to capture all the key strokes of an infected machine. The individual used the key logger to capture the credentials of employees and to subsequently extract sensitive trade secrets. In addition to the intellectual property, documents containing personal information on employees and senior executives was also stolen. The individual used one of the accounts to create a physical access badge to gain continued access to one of the facilities and retrieve devices placed onto the network.

  Tom's Takeaway: Physical security is often overlooked as being critical in the security of digital information. We educate our clients that physical security is the basis on which all other logical controls are built. As you do your risk assessments, I encourage you to account for the physical aspect. Are key systems restricted to authorized personnel, are monitors positioned away from public view, is physical entry logged and monitored? These are some of the significant questions to consider.

- **A new offering circulating in the Dark Web and cyber underground has been identified by researchers.** It is known as Disinformation-As-A-Service (DAAS). Similar to the tactics used by nation states to sway public elections, the service is being offered to private companies to either create positive propaganda about themselves or negative propaganda about rivals. The cost of the service is priced competitively at a few hundred dollars. In addition to targeting the social media platforms to spread the information, the service will also include creation of articles, blogs, websites, etc.

- **Best Western International was identified by security researchers as exposing customer booking details in an unsecured cloud storage system**. The reservation management systems, AutoClerk, had an exposed database that included the personal information on more

than 100,000 individuals, including U.S. government and military personnel. The exposed information included user credentials, name, date of birth, address, phone number, dates of travel and masked credit card information. For select records, the information also included the hotel, room number and check-in time. The government and military information was exposed as a result of a contractor using the reservation system to book travel arrangements on behalf of the government.

- **Security researchers have identified approximately 21 million credentials for sale in the Dark Web belonging to Fortune 500 companies.** 76% of the credentials were exposed in the last 12 months.

  Tom's Takeaway: The market for stolen credentials extends much broader than just the Fortune 500 companies. Credentials are compromised and sold for businesses of all sizes, including individuals. With the credentials in hand, the attackers will leverage that information knowing that people have a tendency to use the same password or close variation thereof across sites. To help protect our clients, we offer a Dark Web monitoring service that will continually attempt to locate these compromised credentials and notify the customer of what accounts have been identified. This helps create invaluable situational awareness to the exposure of the company in the Dark Web and ensure a proactive response. If you would like a complimentary Dark Web check for your business e-mail domain, please contact me directly.

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.