Cyber Roundup – May 2019

By Thomas J. DeMayo, Principal, Cyber Risk Management

Imagine if your organization were subjected to any one of the cyber infiltrations reported in this month's *Cyber Roundup*. If you can relate to any of the incidents, now is the time to call PKF O'Connor Davies to see how we can help avoid putting your business at cyber risk.

Key Cyber Events

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

- Educational institutions made the headlines last month as a result of various cyber incidents, be it from students or malicious external cyber attackers. The key events are as follows:

  - **Two students of New Jersey's Secaucus High School performed a "denial of service" attack against the school's wireless network in order to avoid taking an exam.** With the school's curriculum reliant on the internet, taking down the network resulted in students being unable to access their coursework, inclusive of the exam the attackers were trying to avoid.

  - **California's Berkeley High School experienced a hack of their first-ever student government elections.** One of the candidates attempted to rig the election by casting numerous online votes for themselves. The student conducting the hack leveraged a weakness in how the school assigns default passwords to students, effectively making the default password the student ID.

  - **College of St. Rose in New York was the victim of a former student that walked around and inserted a malicious USB device into computers, destroying 59 devices.** The suspect videotaped himself committing the acts. The malicious USB device was purchased online and effectively caused lethal power surges that destroyed the machines. The incident resulted in damages amounting to approximately $51,000.

  - **Georgia Tech experienced a breach as a result of web application vulnerability that resulted in the potential exposure of 1.3 million current and former employees, students and applicants.** The information included personal information, inclusive of social security numbers. Georgia Tech is actively investigating the issue.

Tom's Takeaway: Educational institutions will continue to be a target. In our experience, educational entities try to promote an open and collaborative atmosphere, often times at the expense of security, assuming they can have the best of both. Our mission is to inform not only the educational institutions but also the readers of this *Cyber Roundup* that you can have both an open atmosphere and security. Processes may need to be re-engineered and staff educated, but it is certainly doable. We try to shift our client's perception that security is not always about saying "No," but to saying "Yes" with alternative and more secure approaches.

- Security Vendor Malwarebytes reported that ransomware events impacting commercial entities increased 189% since Q4 of 2018 and 508% since Q1 of 2018. These statistics should come as no surprise to our *Cyber Roundup* readers. While we reported on a number of entities that were impacted in March, that trend continued in April. The following key ransomware events occurred during April:

  - **Arizona Beverages suffered a ransomware attack that impacted hundreds of systems and halted sales operations.** The ransomware message displayed on the impacted machines included the Company's name, indicating a targeted effort. When the incident occurred, it was identified that the backup system in place wasn't configured correctly to retrieve the backups in a timely manner.
  - **Garfield County, Utah suffered a massive ransomware attack, knocking the systems offline for weeks and ultimately resulting in the County having to pay the ransom to obtain access to their systems and data.** The ransomware infection was the result of a user falling for a phishing e-mail.
  - **The Weather Channel suffered a ransomware attack taking the live TV program off the air.** The station was only down for approximately an hour. Fortunately, The Weather Channel had appropriate backup mechanisms in place and was able to recover and resume operations in a short period of time.
  - **The City of Stuart, Florida suffered a ransomware attack impacting operations.** The City of Stuart refused to pay the ransom. Fortunately, a viable backup existed from which it could be restored. As with Garfield County, the attack was started by way of a phishing e-mail.

- **WiPro, a global IT systems consulting company, suffered a breach of their systems.** The attackers who obtained access were focused on targeting WiPro's client base. Servicing a multitude of clients, including many Fortune 500, WiPro is a target-rich environment to carry out supply chain type of attacks. Based on the investigation thus far, reports indicate that the attackers were sophisticated and well prepared. The investigation remains ongoing.

Tom's Takeaway: As businesses increasingly rely on third parties to operate, enhance, and grow their business, attacks against the supply chain are only going to increase. Attackers actively search for the weak links in the security chain, and many times that link is a third party. The only way to address this threat is to ensure that you have a process in place to assess the security posture of any third party you interact with that can pose a direct or indirect threat. Incidents will always occur, but the question to ask yourself is can you demonstrate to your stake holders that reasonable measures were taken to understand and manage the third party risk.

- **Genesis, an invite-only cybercrime marketplace on the dark web, was identified as offering approximately 60,000 stolen profiles including credit card details, browser fingerprints, user credentials, etc. ─ collectively referred to as the "digital identity."** This information is obtained from victims infected with specific malware designed to steal the information and send it to the Genesis operators. With identities ranging in price from $5 to $200 dollars, what makes the offering unique is the ease in which purchasers of the identity can use the information. Genesis will provide a Chrome bowser extension that will allow the purchasers to simply import the purchased identities and access the web resources to which the identity granted access. Because of the type of detail included in the stolen identities, it allows the user of the identity to potentially fool online anti-fraud systems designed to detect abnormal account login activity.
- **Saint Ambrose Catholic Parish in Brunswick, Ohio was the victim of a $1.75 million business e-mail compromise**. To accomplish the hack, the attackers obtained access to two e-mail accounts belonging to the church. Once access was obtained and insight into pending transactions was learned, the criminals posed as a hired construction company and instructed the church employees to update their banking information for the construction company. The theft went unnoticed until the construction company contacted the church inquiring of the late payment. In April, the FBI's Internet Crime Center published their annual Internet Crime Report. The report noted that business e-mail compromise, such as what occurred to Saint Ambrose, hit 1.2 billion in 2018, up 675 million from 2017. Saint Ambrose is just one of many victims impacted by this type of attack.

Tom's Takeaway: While a company can never prevent the receipt of business compromise e-mails, they can implement a multi-layered approach internally to prevent the fraudulent transfers from completing. Core to our assessment approach, we always confirm that our clients are structured to avoid a business e-mail compromise event. If you would like to learn more, please feel free to contact me.

- **Steps to Recovery, a Levittown, PA based addiction treatment facility, suffered a breach exposing approximately 5 million records containing patient information.** The exposed records were identified in an unprotected database accessible from the internet. The security researcher notified Steps to Recovery of the leak and the database was taken offline. Steps to Recovery is currently investigating the incident to determine if patients need to be notified.

- **EmCare, a Dallas based provider of outsourced physician services to hospitals across the U.S., reported a breach to their e-mail system.** It was alerted that an unauthorized individual obtained access to a set of employee e-mail accounts. The accounts contained various types of personal information on employees, patients and contractors. The breach is believed to impact 60,000 individuals, 31,000 of whom are patients.

- **In an April briefing, Mike Pompeo, U.S. Secretary of State, confirmed that depending on the circumstances, a cyberattack against Japan could result in a U.S. response.** The U.S. is obligated to protect Japan as a result of the U.S.-Japan security alliance ratified after World War II.

- **Microsoft alerted that it suffered a data breach impacting their web based e-mail services such as Outlook.com, MSN.com and Hotmail.com.** The attack, which was the result of a support agent's compromised credentials, is believed to have lasted for three months (January 1st to March 28th) prior to being detected. Microsoft claims that the credentials would only allow the hacker to view account e-mail addresses, folder names and subject lines of the e-mails. The content of the e-mail and attachments were not accessible. The number of accounts impacted has not been disclosed. Microsoft has notified potentially impacted customers and, as an additional layer of protection, is advising those impacted to change their passwords.

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.

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.