Cyber Roundup – June 2021

By Thomas J. DeMayo, Principal, Cybersecurity and Privacy Advisory

Cyber-related crimes are a global threat. As we celebrate graduations this month, it's no surprise we see a prominent college cap and gown seller suffer a credit card breach. With the world becoming more interconnected and technology moving at a supersonic pace, everyone shares in the responsibility of securing cyberspace. As quickly as a program to prevent cyberattacks is created, criminals have figured out how to breach those safeguards. Often these attacks could have been prevented by simple solutions. Solutions that PKF O'Connor Davies can help you identify and implement.

Key Cyber Events

The following is a rundown of what happened during the month of May 2021. We welcome your comments, insights and questions.

- **Biden signs executive order to strengthen U.S. cybersecurity.** On the heels of the Colonial Pipeline attack, President Biden took steps to strengthen the United States cybersecurity defenses. This breach was just the latest in a series of threatening attacks compromising sensitive data. Biden's executive order takes several steps aimed at modernizing the nation's cybersecurity, including:
  - Requiring IT service providers to alert the government to any security breaches while removing contractual barriers that may have prevented this in the past.
  - Creating a standardized federal cyber incident playbook.
  - Forcing the government to upgrade secure cloud services, infrastructure and implementation of multifaceted authentication and encryption.
  - Improving security software sold to the U.S. government.
  - Establishing a "Cybersecurity Safety Review Board."
  - Improving information sharing with the federal government.

- **The FBI's Internet Crime Complaint Center (IC3) sees 100% increase in cybercrime complaints over the past 14 months.** IC3 began monitoring cybercrime complaints in 2000. At that time, it took seven years to reach 1 million complaints. More recently, between March 2020 and May 2021 due to the pandemic, the IC3 logged one million complaints. The report states "… while the American public was focused on protecting our families from a global pandemic and helping others in need, cyber criminals took advantage of an opportunity to profit from our dependence on technology to go on an Internet crime spree." The top three crimes reported were phishing, non-payment/non-delivery scams and extortion. However, victims' monetary losses were greatest in Business Email Compromise (BEC) scams, romance scams and investment fraud.

- **HAECHI-I, an Interpol operation, intercepted a total of USD $83 million from financial cybercrimes.** This six-month (September 2020 through March 2021) international joint-effort operation, which initially focused on the Asia Pacific region, soon spread to every continent due to the borderless nature of online attacks. Of the over 1,400 investigations opened, many are still ongoing; however, 892 cases were solved. Over 1,600 bank accounts were frozen, and 585 individuals were arrested. Most of the victims' funds were recovered as law enforcement froze the accounts used by these crooks. This investigation focused on international financial crimes, which according to the report, easily targets victims in various countries due to the borderless nature of the Internet. Operation HAECHI-I proves, once again, cyberattacks are global in nature and that close intercontinental collaboration is the only way to fight these criminals.

Tom's Takeaway: The news is often flooded with all of the negative cyber events while the positive is sometimes lost in the noise. It is important to remember that law enforcement is actively working to try to address cyber threats; however, it is equally important to understand the sheer enormity of this problem and the difficulty of making the smallest of dents in the cybercriminal world. Law enforcement can't win this battle alone, we all have a role that we need to play – from protecting our home and corporate networks, sharing intelligence, and notifying when we are victimized.

- **147,000+ Scripps Health patients and staff personal information at risk due to malware attack.** On May 1, Scripps Health took their systems offline as they announced an "unauthorized person" had accessed their network, acquired personal data and then deployed ransomware. Scripps notified over 147,000 individuals affected suggesting they take steps to secure their information. The health care system is providing complimentary credit monitoring and identity protection services for those whose Social Security and driver's license numbers were compromised. Scripps began a time intensive, broad manual review process that will delve into who exactly has been affected. It's also enhancing information security and technology systems to prevent any future attacks. One month after the attack, Scripps electronic health record system was finally back online and patient appointments, records and activities are getting back to normal. According to Scripps, patient care was never affected.

- **Cancer software security breach hits 40 health systems.** Elekta, a cancer care software company that provides linear accelerators for radiation treatment to many health systems, was the firm impacted by this breach. Victims were forced to alert patients to treatment interruptions due to the incident. This broad-based attack forced health care facilities to reschedule life-saving radiation treatment to many patients. The attack was first discovered on April 6 and all services were restored by April 9. There is no evidence of any compromised patient information.

- **19 petabytes of data exposed across 29,000+ unprotected databases leaving data exposed to anyone, including threat actors.** Databases, where sensitive information is stored, are prime targets for threat actors who frequently don't even need to hack a system to gain precious data. Much of this data is left unsecured which allows access without any identifying information – no username or password is needed. Within the past year, data leaks from "open" databases have decreased, and *CyberNews* wanted to find out how many databases are still unsecured. They found that given the current heightened cybercrime environment it is astonishing how many databases are still left unsecure. Their investigation used specialized search engines to scan for "open" databases. Millions – if not billions – of users are at risk with just a click of a button. Globally, China ranked first by a large margin in vulnerability and the United States came in second.

  In 2020, thousands of unsecured databases were wiped out by a "Meow" attack. Shocked owners, who were not asked for a ransom nor given any explanation, were left with empty file folders named "Meow," the attackers calling card. In the end, it appears these attacks were simply for fun as anyone can easily find these unprotected clusters by using Internet of Things (IoT) search engines. Even more surprising is that a year later, 59 of the original victim databases are still unprotected. It is more important than ever to continue raising awareness about exposed and publicly accessible databases. Unfortunately, many databases are managed by untrained administrators making them easy targets. There are many simple steps that can be taken to secure your database against these threat actors.

- **Prominent college cap and gown seller suffers credit card breach.** Graduating students from across the United States report fraudulent activity after using credit card payments with Herff Jones. While the firm has launched an investigation to assess the scope of the data breach, Herff Jones was entirely unaware of this violation until students began to complain about fraudulent charges ranging from $80 to $1,200. Although the exact date of the breach is unknown, early deceptive transactions began with products purchased in April.

- **SmileDirect shares decline 7% after cybersecurity breach, resulting in a $10–15 million financial impact this quarter.** While the company stated "no ransom was paid," it did not specifically quantify the nature of the attack. However, their statement suggests it was indeed a ransomware incident. They further stated they were not aware of any data or other loss of assets,

including customer or team member information. Given the huge financial loss, SmileDirect is hopeful insurance coverage will help defray the lost revenue.

Tom's Takeaway: A cyber event can have a devastating impact on a business. While loss of revenue and expenses related to the event can be calculated, the reputational impact and loss of customer trust is impossible to quantify. That trust is more often than not the biggest intangible asset on the company's books. If you need assistance in preserving that Trust, we can help.

Ransomware

Ransomware attacks are happening everyday it seems – from municipalities to private companies, to health care systems. No one is exempt from these bad actors and the damage and disruption they cause. In most cases, these attacks are reported to the FBI who investigates the genesis of these attacks and discourages any ransom be paid. However, very often these extortion requests are negotiated, and a payment is made to facilitate recapturing the data and/or getting systems up and running once again.

From the dark side of things, the cyber-underground has made big business of building programs and selling samples to threat actors who are willing to pay anywhere between $300 to $4,000 for ready-to-use attacks or ransomware-as-a-service rentals which can cost $120 to $1,900 per year. Regardless of how it happens, an attack can leave your organization helpless and beholden to cybercriminals until their demands are met. In many cases, these attacks could have been prevented had the victim invested in updating training and protocols or buying much needed cybersecurity updates. We here at PKF O'Connor Davies can always help you **Know Better Cybersecurity.**

Contact Us

Thomas J. DeMayo, Principal, Cybersecurity and Privacy Advisory
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, fourteen offices in New York, New Jersey, Florida, Connecticut, Maryland and Rhode Island, and more than 1,000 professionals, the Firm provides a complete range of accounting, auditing, tax and management advisory services. PKF O'Connor Davies is ranked 27th on *Accounting Today*'s 2020 "Top 100 Firms" list. It is also ranked among the top 20 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.