Cyber Roundup – July 2021

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

Ransomware gangs do not, and will not, discriminate as to their targets. Everyone at this point needs to have a solid plan in place to not only prevent a ransomware attack, but also how to respond should one occur. While many have – and continue to count on – cyber insurance to be their saving grace, the insurance landscape is shifting. The days of easy to find and obtain cyber insurance are quickly disappearing. We are not only seeing a dramatic increase in premiums, but the requirements to be eligible for such insurance are also more extensive. If you want to be insured going forward, you will first need to prove that all aspects of your cybersecurity and related policies are healthy. If you need assistance in ensuring that your business is in good cyber health, give us a call. **Know Better Cybersecurity.**

Key Cyber Events

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

- **The Department of Justice alerted that executives should prepare for an "exponential" increase in ransomware attacks.** Lisa Monico, the Deputy Attorney General, made it clear that business leaders need to do more to defend against ransomware attacks. Further, Anna Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology, issued a memo to business leaders reminding them they have a "critical responsibility" to protect their businesses. The memo can be found here.

- **The following ransomware events took place in June:**

  - JBS, a meat processing provider, suffered a ransomware attack that resulted in the shutdown of several processing plants in the U.S. JBS was successful in restoring their systems; however, they ultimately paid $11 million in crypto currency to prevent the leakage of exfiltrated data by the ransomware group.

  - The New York Law Department suffered a ransomware attack disrupting legal proceedings as legal counsel was unable to access data related to cases and hearings. The attack was the result of a compromised credential of an employee that was used to access the systems. It has not been confirmed if data was also exfiltrated. The FBI is investigating the matter.

  - The City of Tulsa alerted that 18,000 of its files had been posted on the dark web as a result of a ransomware attack in May. The files mostly consisted of police citations and other internal files. As of this writing, Tulsa is the 37th municipality that suffered a ransomware attack in 2021. The year 2020 saw 113 municipalities impacted by ransomware.

  - Des Moines Area Community College suffered a ransomware attack that disrupted operations for over a week. The attack impacted the online instruction systems and telephone network.

  - The Massachusetts Steam Ship Authority that operates ferries equipped to carry cars between Cape Cod and Matha's Vineyard suffered a ransomware attack. The attack disrupted operations, taking down their website. The ransom was not paid, and it is believed no sensitive information was taken.

- **Cloud hosting provider iland issued a report** noting that only 54% of organizations have a company-wide disaster recovery plan, with only 50% testing the plan.

  Tom's Takeaway: In a landscape plagued with ransomware, disaster recovery is critical. One of the more frequent observations we have when doing our risk assessments is the lack of a disaster recovery and business continuity plan. Many businesses falsely assume that disaster recovery is a purely technical issue. What they don't realize is that disaster recovery is only a subset of the overarching business continuity plan. As with information security, this is a business issue that requires the assistance of a technical solution. If you need assistance in developing your business continuity and disaster recovery plan, we can help.

- **A vendor of CVS exposed 1 billion records of the Company's healthcare data.** The exposure was the result of an incorrectly configured database accessible from the internet. The database was accessible with no password. The exposed data consisted of search data entered into cvs.com and cvshealth.com. In most circumstances, the data attributes exposed did not directly contain identifiable information; however, a collection of e-mail addresses was contained in the breached dataset. The issue was corrected immediately upon notification of the discovery.

- **Mercedes-Benz USA reported that a vendor utilized by the Company exposed 1.6 million records as a result of a cloud configuration issue.** The data contained such information as names, e-mail addresses, phone numbers, and information on purchased vehicles. For a smaller subset, approximately 1,000 individuals, highly sensitive information such as credit score, drivers' licenses, credit card, and social security numbers were exposed.

- **Wegmans Food Markets notified customers of a breach as a result of two cloud databases used by the Company that were incorrectly configured and accessible to anyone.** Information exposed consisted of name, address, phone numbers, birth dates, shopper club member numbers, and the username and password associated with customers' Wegmans.com online account.

  Tom's Takeaway: Security issues aren't always the result of a malicious external threat actor, but often the result of a mistake by a trusted party. When doing a security assessment, your assessor should look for issues that cannot only be leveraged by the malicious outsider, but issues that also exist because of misconfigurations by personnel or poor internal practices. Mistakes happen. When we do our assessments, we have one goal: identify anything and everything we can before something or someone can take advantage and impact the business.

- **74% of new malware identified in Q1 of 2021 was classified as zero day malware, reaching a new record high.** Zero day malware is the highest risk malware as it exploits or takes advantage of previously unknown vulnerabilities, meaning, it cannot be easily prevented or detected in many circumstances. The term "zero day" has been coined because the vendor of the vulnerable product is only just learning of the issue and has "zero days" to correct it.

- **The NY Metropolitan Transportation Authority was breached by Chinese threat actors.** The threat actors utilized a zero day exploit that existed for their remote access gateway. The threat actors obtained access to the system for several days and successfully compromised three of the MTA's 18 core systems. The attack was ultimately stopped with coordination by federal and state agencies. No information was stolen or system configuration changes made by the threat actors.

- **Six Flags Great Adventure was ordered to pay $36 million in the settlement of a class action lawsuit.** The lawsuit was the result of Six Flags collecting visitor fingerprints upon entry to the parks. The suit claimed that Six Flags, in the course of the collection, violated Illinois' Biometric Privacy Act that requires any collector of biometric data obtain written consent from the person and provide notice as to why and how that data will be processed. Six Flags provided no such notice or obtained consent. As a result of the settlement, anyone who had their finger scanned between October 1, 2013 and April 30, 2016 can receive up to $200.

  Tom's Takeaway: If you operate a business that results in the collection and processing of personal information, it is critical that you not only have the correct security personnel to protect that information but the correct privacy personnel as well. Information security and privacy are two fundamentally different skillsets. To avoid any issues such as Great Adventure, you need to fully understand the type of personal information you collect and the privacy laws that may apply

based on the state of operation or state of residence of the impacted person(s). At PKFOD, we provide **Know Greater Privacy and Cybersecurity** advisory services. If you need assistance, please contact us.

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.