Cyber Roundup – August 2021

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

As you may be aware, PKF O'Connor Davies specialists from various disciplines, including our IT consultancy practice, serve as the vCISO (a.k.a. virtual Chief Information Security Officer) for many outside businesses. This gives us the vantage point and hands-on experience to develop and leverage IT best practices. In this issue of the *Roundup*, you will learn about cyber events that occurred last month and specific actionable practices. In some cases, we have also provided associated links that can help you with:

- Securing potential vulnerabilities, including patch management
- Expanding risk assessment to key business units
- Risks to wireless networks jeopardizing mobile workforces
- Ransomware threats and mitigation
- Independent assessment of your managed service provider (MSP)
- Lawsuits against companies that had undergone ransomware attacks

Key Cyber Events

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

- **The Cybersecurity and Infrastructure Security Agency (CISA) published the top 30 vulnerabilities targeted by cyber criminals in 2020 to date.** The CISA worked **in** combination with the FBI, the Australian Cyber Security Center, and the UK's National Cyber Security Center. The posting can be found here. All the vulnerabilities posted have fixes available from the vendors.

- **In a report released by Trend Micro, 22% of exploits for sale in the cyber underground are for vulnerabilities more than three years old.** An exploit is the piece of code that allows a vulnerability to be leveraged.

  Tom's Takeaway: The prior two bullets underscore the importance of a strong patch management program. The program must be designed to identify, distribute, and monitor the successful installation of the patches deployed on a timely basis. For the businesses that I am the vCISO for, we hold at a minimum bi-weekly meetings to review the patch deployment status. I encourage you to take the list provided by CISA and verify with your IT department that the issues identified do not exist in your environment. If you need assistance in validating the effectiveness of your program, please feel free to contact us.

- **Facebook reported that they shut down approximately 200 fake accounts belonging to Iranian hackers that focused on spying on U.S. aerospace and other military officials.** The hackers created the persona of a female aerobics instructor on the platform to establish a relationship with the U.S. personnel. The interactions lasted over the course of months and resulted in the targeted individuals being persuaded to click on malicious links that ultimately installed spyware.

- **The U.S. State Department announced they will award up to $10 million for any information leading to nation state hackers targeting U.S. critical infrastructure.** The announcement notes that includes, but is not limited to, ransomware.

- **Colorado signed into law the Colorado Privacy Act (CPA) making it the third state to pass comprehensive privacy legislation.** The law is specific to the protection of information processed on individual consumers and not in a commercial or employment context. The law will apply to those businesses that operate in Colorado or target residents of Colorado. As with other privacy laws, it will mandate specific protections and disclosures be provided for consumer information.

  Tom's Takeaway: Privacy is an issue that will sooner or later impact your business in a material way. While a comprehensive federal law won't likely be passed any time soon, the states will continue to lead the charge. Think of privacy as a basic right that you as a business have a duty to uphold as it relates to your employees, business partners, and customers. If you need assistance in understanding your privacy obligations and developing a privacy program, please contact us.

- **Food chain, Chipotle, suffered a breach of an account belonging to an e-mail marketing platform.** The account was used to send malicious e-mails to individuals luring them to click on links. The majority of the e-mails were designed to steal credentials; however, a small number also included malicious attachments.

  Tom's Takeaway: When we perform our assessments, we will always risk assess the marketing and communications departments to identify how they manage and secure the systems they operate. It is very common for these departments to utilize shared accounts and weak credentials. More often than not, these departments fly under the radar as it relates to their risk. In my opinion, what better group to target than the group that holds the keys to the reputation of the business and the relationships with their customers and business partners. If your current cyber assessments are IT-specific only and don't factor in the key business units, a large piece of the puzzle is missing. If you need assistance in finding and filling those puzzle pieces, we can help.

- **The National Security Agency (NSA) published an alert regarding the risk that wireless networks pose to teleworkers.** The NSA provides a cheat sheet [can be found here] that gives best practices and awareness as they relate to public wireless, Bluetooth, and near field communications (e.g., read your credit card by being in close proximity). I encourage you to read this document and provide it to your IT team to identify if any additional controls should be implemented to protect your remote and/or mobile workforce.

- **Ransomware continues to be an evolving threat.** To combat the issue, the Cybersecurity and Infrastructure Security Agency (CISA) deployed the stopransomware.gov website. The website is a "whole-of-government approach that gives one central location for ransomware resources and alerts." The website is designed to empower organizations to "understand the threat of ransomware, mitigate risk, and in the event of an attack know what steps to take next". The website can be found **here.**

- **The following are the key ransomware events for July:**

  - Kaseya, an IT solutions provider for IT Managed Service Providers (MSPs), suffered a breach as a result of software flaws in their platform that resulted in approximately 1,500 organizations being infected with ransomware. The impacted organizations were customers of IT MSPs that utilized the platform to monitor and manage their networks. The ransomware group responsible for the hack, REvil, demanded $70 million to restore access to the impacted networks.

    Tom's Takeaway: IT MSPs play an important role in managing and protecting many organizations; however, they are also key high risk vendors relating to your security. While they play a role, it is critical that you ensure that your IT MSP also has a well-defined information security program and has the appropriate controls and processes to protect your organization. One of the biggest mistakes organizations make is allowing their IT MSP to perform the risk assessments of the organizations in which they manage. Coming from an audit firm, that is a big no-no. Asking an entity to self-assess and provide meaningful unbiased feedback is a recipe for failure. For the investment made in that type of relationship, obtaining **independent** feedback is one of the safest ways to protect that investment and the business.

- Retailer, Guess, disclosed a data breach after a successful ransomware attack in February. The attack resulted in the exfiltration of approximately 200GB of data that included sensitive personal information such as SSN, driver's license, passport, and financial account numbers.

- In an article published by the Washington Post, companies that have suffered ransomware attacks are now being sued by consumers and workers that claim to have suffered harm as a result of the insufficient security practices. To do the article justice, I suggest you read it – found here. If such a practice becomes common and precedent is set, the ramifications of not having a sound security program will become that much greater.

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.

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.