Cyber Roundup – July 2020

By Thomas J. DeMayo, Principal, Cyber Risk Management

The last bulleted news item in this month's *Roundup* speaks to a breach resulting from password mismanagement. I fully appreciate how frustrating passwords can be. It is in this frustration of managing multiple passwords that people by nature take a somewhat lax approach to securing those passwords and ultimately end up placing themselves at risk.

If you haven't done so already – and bearing in mind the adage *Those who can, do, and those who can't, pay* – I offer the following simple yet highly effective tips to better manage your passwords.

1. Use a passphrase or a sentence. It is easy to remember and the longer the better.
2. Leverage multi-factor authentication (verifies user's identity by requiring multiple credentials – not just user name/password). Most major online platforms support it at this point.
3. Use a password manager (there are many of them out there – some free, others charge fee.) Why struggle with remembering multiple passwords when technology exists to remember it for you?

How far we have come from ***Open Sesame*** used by Ali Baba to access hidden treasure. Same principle, more rules.

Key Cyber Events

The following is a rundown of what happened during the month of June 2020. We welcome your comments, insights and questions.

- **Security researchers discovered 28,000 spear phishing websites created by a hacker for hire group dubbed "Dark Basin."** Spear phishing is a type of phishing that is very targeted to the specific recipient to increase the potential for success. The websites target individuals and institutions across all industries, including advocacy groups, hedge funds, journalists and elected officials.

Tom's Takeaway: The cyber underground has created a number of different business models catered to the needs of individuals and businesses ***that want to perform cyberattacks.*** The benefit of the cyber realm is that attribution becomes difficult and creates a perception of safety and separation from those commissioning the attacks. On a protective note, with sufficient and effective cyber awareness training, anyone can prevent becoming a victim. If you need assistance in performing cybersecurity training, please contact us.

- **A hacking group, dubbed "Distributed Denial of Secrets," published approximately 296GB of data stolen from over 200 police departments and fusion centers.** The data, which spans approximately 24 years, has been broken down into 13 categories such as images, financial information, audio, etc. It is believed the breach occurred as a result of a common web developer and platform. Although the group "Distributed Denial of Secrets" published the data, the infamous hacking group "Anonymous" has claimed to be the source of the attack.

Tom's Takeaway: Third-party risk when utilizing any shared and common platform will only continue to increase. What is critical is performing proper due diligence of the third-party service organizations you utilize. The fundamental problem and challenge that we see, is that many organizations are in fact embracing third party due diligence; however, the service organizations are utilizing low cost and unqualified providers to test their cybersecurity posture. While the service organization can effectively attest to having performed the testing, **the quality of the testing remains unchecked and hidden.** In this specific issue that caused the breach, we do not know what, if any, testing was performed. However,

understanding the nature of the breach, we can say with confidence that a qualified web penetration tester would have likely identified the issue to allow for remediation.

- **Three higher education institutions were targeted and succumbed to ransomware during a one-week period in June.** The impacted entities consisted of Columbia College in Chicago, Michigan State University, and University of California in San Francisco. The three attacks all involved the "Netwalker" family of ransomware which not only encrypts the data, but also exfiltrates and threatens to publish the stolen data if the ransom is not paid. The University of California in San Francisco paid $1.14 million to regain access to their files. Michigan State has claimed they refused to pay the ransom, and it is unknown if Columbia College ultimately paid.

- **The city of Florence Alabama suffered a ransomware attack in which $300,000 was paid to recover the impacted systems.** The impacted systems and data included that of employees and constituents. The city was alerted by a security researcher prior to the incident that their machines had been identified as being compromised and while the city took action to try and prevent the incident, it was not enough.

Tom's Takeaway: Municipal entities continue to be a favorite of ransomware gangs. This is unlikely to change. We believe there will be an increase in the coming months and year as most municipalities will be experiencing budget cuts due to the pandemic. Prior to the pandemic, municipal spending in cyber space was minimal; the pandemic will only exacerbate the issue. If you are employed by a municipality, we encourage you to support the performance of an assessment of the municipality's cybersecurity posture and implement a strategy on how to effectively defend it in a cost-effective manner. If you need assistance, please contact us.

- **The carmaker Honda reported a ransomware attack that impacted its operations across multiple countries.** Honda has claimed that no customer data was compromised as a result of the attack. The attack occurred on Monday, June 8, 2020. Honda was able to restore operations by Tuesday, June 9. The attack appears to be tied to the SNAKE ransomware variant which is designed to impact industrial control systems.

Tom's Takeaway: Back in the day, a partner of the Firm instilled in me the wisdom of the five P's: **P**roper **p**lanning **p**revents **p**oor **p**erformance. This truism applies to many areas of life, including the cyber realm, and Honda demonstrates that. They clearly had the necessary protocols in place to recover and had planned for such an event. Every organization should embrace the five P's and prepare for an incident to occur. When it comes to ransomware, **the silver bullet is the plan** you have in place to recover should it happen.

- **A $5 billion class action lawsuit has been filed against Google under the allegation that Google is collecting and processing users' browsing information when they utilize incognito mode.** Incognito mode is an option in Google chrome that is supposed to provide private browsing. It alleges that Google itself uses the information obtained to learn about user private browsing habits.

- **Nintendo issued an alert that approximately 300,000 online customer accounts may have been breached since April 2020.** The cause of the breach is unrelated to any technical issue with Nintendo's online platform; however, it is the result of its customers reusing their passwords across multiple accounts. Such a tactic is referred to as "Password Stuffing."

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, twelve offices in New York, New Jersey, Connecticut, Maryland and Rhode Island, and more than 800 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.