Cyber Roundup – August 2020

By Thomas J. DeMayo, Principal, Cyber Risk Management

As you can see, cybercrimes go on – pandemic or no pandemic. It's way too early to start opining on what the historical, economic, cultural and social effects it will have on our lives. We know for sure, however, that computer technology has made more than a small contribution to "life as we know it." It's easy to say use this time to upgrade, improve and secure your business and personal computer technology; nevertheless, our dependence on it is paramount. So, don't hesitate to reach out to us.

Key Cyber Events

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

- **The SEC's Office of Compliance Inspections and Examinations (OCIE) issued a Risk Alert related to ransomware.** The Alert notes that there is an increase in both the frequency and sophistication of ransomware attacks targeting financial institutions. Further, the Alert notes the increased targeting of service providers by the cyber attackers. The Alert can be viewed here and offers key measures any company can adopt to protect themselves against ransomware.

- **As OCIE noted, the ransomware threat is escalating; however, the threat is much broader than financial services.** The following are ransomware events which occurred in July:

    - Blackbaud, one of the leading providers of software solutions to nonprofits, suffered a ransomware attack. Although Blackbaud was able to contain the incident, a subset of data was successfully stolen by the cyber criminals prior to containment. Blackbaud was able to successfully recover; however, they ultimately paid the ransom under the condition that the cyber criminals would delete the data they had stolen. The data stolen has been reported by Blackbaud not to contain any highly sensitive data such as SSNs or financial numbers. A more detailed summary of the incident can be found on the Blackbaud website, here.

    - Garmin, a provider of GPS technology, suffered a ransomware attack that impacted many of its systems and services utilized internally and by millions of its customers. While not confirmed, reports are currently indicating that a multi-million ransom was paid to restore access to the impacted systems. Garmin has reported that sensitive customer data was not compromised.

    - Collabera, a New Jersey-based provider of IT services and staffing, suffered a ransomware attack. Collabera was able to restore their systems without paying the ransom; however, the attackers managed to steal sensitive data related to their employees such as SSNs, passport, visa information, etc.

Tom's Takeaway: Ransomware is a threat that we will continue to see in the future. What is important to appreciate is that every company is a target. From the Fortune 500s with large security teams and budgets, to the small businesses with limited IT resources. Regardless of size, the impact can be devastating. Of particular concern is that the ransomware events of the past that just focused on encryption are long gone. The stealing of data has become common place to give the attackers another bargaining chip in their request for payment. While a cyber incident can never be guaranteed not to occur, a significant amount can be done to prevent the occurrence or respond effectively should it manifest. If you need assistance on how to create and maintain an effective cybersecurity program, please contact us.

- **Brian Krebs of KrebsOnSecurity published a very interesting article on business identity theft**. In his article, he highlights the dramatic increase in business identity theft noted by Dun & Bradstreet as increasing 100 percent during 2019, and, not surprisingly, 258 percent in 2020. While we often focus on personal identity theft, business identity theft is also a major concern. Scammers will go as far as engaging image editors to fabricate official documents that are tied to the business, such as tax records or utility bills, and setting up fake websites. After establishing a fraudulent profile with Dun & Bradstreet, they will begin to open up lines of credit in the businesses name. During the pandemic, they have increasingly focused on small businesses that are still active and exist. Dun & Bradstreet has offered their own guidance on the attack and key considerations for a business to follow. We highly recommend you review the article here to protect your business.

- **The U.S. Secret Service announced the combination of their electronic and financial crimes unit into a new Cyber Fraud Task Force.** The new task force will focus on the investigation and prosecution of cyber-related attacks such as ransomware and business e-mail compromise.

- **The U.S. Secret Service sent out a U.S. private sector and government notification.** It alerted to the increased targeting of IT managed service providers to facilitate ransomware, point of sale intrusions, and business e-mail compromise attacks.

Tom's Takeaway: The role of the IT managed service provider (MSP) is without question a key player in the marketplace in their support of businesses. What we often see, however, is that the business using the IT MSP has done very little research on the security protocols of the IT MSP, and has in large part made their decision on the usage of the IT MSP based on the economics of their proposal. For any business using an IT MSP, it is critical that you ensure they have implemented the necessary best practices to protect your business and will not be the weak link in the chain. If you need assistance in assessing your IT MSP, please contact us.

- **The City of Boston is the latest government entity to ban the use of facial recognition technology.** The decision was largely made due to the high level of inaccuracy of the technology. Based on a study by the National Institute of Standards and Technology, current facial recognition software is up to 100 times more likely to misidentify darker skinned individuals. An MIT study in 2018 came to the same conclusion regarding the high error rates associated with darker skin individuals.

- **In a report by the U.S. NSA and the British National Cyber Security Centre, Russian Intelligence Service sponsored hacking groups have been identified as targeting institutions involved with COVID-19 vaccination research in an effort to steal the information.** The hackers typically utilize publicly-known exploits to gain a foothold, and once inside the organization, they deploy a custom piece of malware to exfiltrate data.

- **Twitter announced a breach that resulted in the compromise of various high profile accounts such as Jeff Bezos, President Obama, Joe Biden, Elon Musk, Mike Bloomberg, et al.** The hacked accounts all tweeted that for every $1,000 sent to a Bitcoin address, $2,000 would be sent back, netting the attack approximately $100,000. A 17-year old Florida teen has been charged with the hack. Details of the incident released by Twitter indicate that the hacker managed to social engineer internal Twitter employees to provide their credentials and gain access to internal systems. Once inside, the hacker would obtain more information about the inner workings of Twitter and further use that information to penetrate deeper into the company. The hacker ultimately gained access to a console that allowed it to reset passwords on the targeted accounts and, if needed, disable the multi-factor authentication they had enabled. Twitter has since secured the accounts and has committed to addressing the vulnerabilities identified.

Tom's Takeaway: Over multiple issues of *Cyber Roundup*, we have emphasized the importance of employee training and communication. This incident again highlights the importance of training. Twitter, undoubtingly, has many sophisticated controls and resources to secure their environment; however, in this situation, all were defeated by targeting the ***human element*** and leveraging the trusted insider. We specialize in employee training and helping companies establish a meaningful security awareness training program. If you need assistance, please contact us.

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.