Cyber Roundup – September 2021

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

While analyzing critical issues to explore in each issue of *Cyber Roundup* and working with our clients on their cyber challenges, I am continually astonished at the schemes bad actors conceive of to disrupt business, the economy and people's everyday activities. I remind myself that both the real world and the cyber world are characterized more by positivity and good intentions, thanks to the invention of the internet. We have a powerful opportunity to add value by supporting our clients and providing them with the knowledge and guidance to confront cyber evil. I'm gratified that the not-for-profit sector, with its mission of improving lives and spreading hope, represents a sizeable part of our Firm's client base. Equally appreciated are the for-profit entities and individuals that supply the public with products and services essential to keeping our economy and its workforce growing.

Our clients, like you, are forces for good and that is why I forge ahead. We are all in this fight together and, therefore, stronger against our cyber foes. As a Firm, we stand ready to support you when needed and help you fight cyber battles when confronted.

Key Cyber Events

The following is a rundown of trends and what's been happening recently. We welcome your comments, insights and questions.

- **Cyber intrusion activity is up 125% in the first half of 2021 compared to the same time last year according to a report issued by Accenture**. The United States (36%), United Kingdom (24%) and Australia (11%) accounted for 70% of the activity and were the three most targeted nations.

  Tom's Takeaway: The continued increase in cyber assaults should come as no surprise. In a "post" pandemic world that is still struggling to find its legs, the continued maturation of cyber crime "as a service" and the relentless efforts by well-organized ransomware gangs, provide all the fuel needed for the increase.

- **Schools have been one of the hardest hit sectors for cyber crime in 2020, costing approximately $6 billion in losses, according to a report issued by Comparitech.** New York, California, Texas and Louisiana lead the states most impacted. Over 1,740 schools were victimized, representing a 39% increase over 2019. Ransomware amounts ranged from $10,000 to over $1 million and schools experienced 7 days of downtime on average and approximately 55 days to recover fully from an attack.

  Tom's Takeaway: It is the responsibility of educational institutions to ensure a safe and effective environment in support of the education of its students. While many schools have focused on the physical threats to students over the years, many have not fully addressed cyber threats. Tackling the cyber threat has and will remain a key component in providing a safe and effective educational environment.

- **In an effort to promote their business, AllWords.Cards, a dark web market place for selling credit card information, provided the information on one million cards for free.** The cards were stolen between 2018 and 2019. The information consisted of all the credit card details that would be needed to effectively carry out a purchase.

- **In a report issued by Kela, the average cost to procure access to companies that have already been compromised is $5,400.** The price appears to be dependent on the revenue of the breached company. The higher the revenue, the higher the ransom that can be demanded.

- **In the ever-changing tactics of cyber criminals, Microsoft identified attackers using Morse code in phishing attacks to evade detection.** The phishing tactics typically included invoice-related lures in a HTML (i.e., web page) attachment. The pages were ultimately designed to steal the victim's user name and password.

- **Microsoft suffered a massive data breach that exposed 38 million customer records, some of which were highly sensitive disclosing a person's SSN, COVID tracing and vaccination information, resumes, etc.** The impacted information was stored in Microsoft's Power Apps Portal. The portal is a platform that allows for the development of web and mobile apps. The issue was the result of a default setting that made public the interfaces to interact with the data. The default setting has since been changed to private.

- **Hundreds of thousands of home routers have been identified as being vulnerable to complete compromise by cyber criminals.** The home routers were mostly created in 2015 or prior. Known cyber threat actors have already been identified as targeting the impacted devices. Devices older than 2015 may be salvageable if the vendor releases an update that can be applied. Older devices will need to be replaced. For a listing of the impacted devices, click here and then scroll to the bottom of the linked article.

  Tom's Takeaway: It is important to remember that the cyber threat persists both at home and in the workplace. While at work, your business will have the primary role of securing your devices; at home, it is entirely up to you. As you introduce more and more internet-connected devices, keep in mind that they periodically will need to be updated to address security threats.

- **T-Mobile has once again suffered a major breach.** The cell phone carrier reported that approximately 49 million customer records had been stolen in their most recent breach. The information consisted of highly sensitive information such as SSNs and driver license numbers. If you believe you are impacted by the breach, you can visit the T-Mobile site here on what to do.

- **The following Ransomware events occurred in August**:

  - The City of Joplin, Missouri suffered a ransomware attack and ultimately paid $320,000 to prevent (hopefully) the leakage of the compromised information. The breach is still under investigation.

  - Ohio-based Memorial Health System suffered a ransomware attack that resulted in surgeries being canceled and patients diverted. While the CEO noted that they reached a negotiated solution to restore operations, the details are not yet available.

  - Ransomware group, LockBit, has been identified as trying to recruit employees or insiders at companies to facilitate the launch of their attacks. The group is offering a substantial payout to those who release a virus within their company.

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.