Cyber Roundup – November 2021

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

As you will see from this month's *Cyber Roundup,* each day bad actors hack systems in industries that range from media to candy companies. Information that is held hostage by cyber criminals until a ransom is paid is more and more prolific and poses an increasingly high threat to privacy and security. Denial of service, phishing, password attacks, ransomware, malware, security breaches, and the list goes on and on.

Staying safe demands expertise and attention. Our experts are here to help guard your firm against any imminent threat or possible attack by bad actors and provide real-time awareness of threats before they occur – priceless.

Key Cyber Events

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

- **NSA Director Paul Nakasone, predicted ransomware-related events will not slow down over the next five years.** According to the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), financial institutions reported $590 million in ransomware-related payments in the first half of 2021 alone. For all of 2020, $416 million were reported. To combat the threat, in an effort spearheaded by the U.S., 30 nations have come together and pledged a shared response to ransomware attacks to ultimately disrupt the ransomware business model. The success of the relationship was clear when the notorious REvil ransomware group was taken offline in October.

  The ransomware-related events are as follows:

  - A survey conducted by ThycoticCentrify identified that out of the 300 IT decision makers who participated, 64% experienced ransomware attacks in the last 12 months and 83% of them ultimately paid the ransom.

  - Accenture, a global consultancy firm, suffered a ransomware event in the summer of 2021. In their most recent filings with the SEC, the firm disclosed that proprietary information was breached as a result of the event. In addition, while it notes that they and their clients have experienced no material impacts to date as a result of the breach and any other cyber-related incidents, it can offer no such assurance that future events may not be material.

  - Ferrara Candy Co., a major candy distributor, suffered a ransomware attack that impacted its production systems and suspended operations in some of its plants. Luckily, the attack did not result in any disruption to the October Halloween candy supply.

  - Cox Media Group acknowledged that a ransomware attack occurred in June that took down its live television and radio broadcast systems. The attack also resulted in the disclosure of sensitive personal information of approximately 800 individuals. Cox did not pay any of the ransom demanded by the threat actors.

  - Manhasset School District in Long Island, NY reported a ransomware attack in September and ultimately did not pay the ransom. Having not received the payment, the ransomware group recently published the stolen information on the dark web. The District

is reviewing the information posted to determine if notifications will need to be provided to any impacted individuals.

- In a new bill entitled, the Ransom Disclosure Act, introduced by U.S. Senator Elizabeth Warren and Representative Deborah Ross, ransomware victims would be required to disclose the following information to the Department of Homeland Security within 48 hours of a ransom payment:

    - The date on which the ransom was demanded.
    - The date on which the ransom was paid.
    - The amount of ransom demanded.
    - The amount of ransom paid.
    - The currency used to make the payment (including type of cryptocurrency, if cryptocurrency was used).
    - Whether the organization that paid the ransom receives federal funds.
    - Any known information regarding the identity of the extortionist

  The intention of the bill is to allow visibility into the payments being made.

Tom's Takeaway: I agree that the ransomware situation will likely continue to get worse before it gets better. What is unfortunate is that the attackers continue to impact such a large number of companies because many still do not have an effective cybersecurity program. It isn't until an incident occurs that businesses ultimately realize that implementing and maintaining a cybersecurity program isn't just nice to have, but is a key business enabler. If you need assistance in developing or assessing the strength of your cybersecurity program, we can help.

- **In a privacy study of several unnamed internet service providers (ISPs) conducted by the U.S. Federal Trade Commission (FTC), it was reported that a treasure trove of personal information is not only collected but shared without disclosure to their consumers.** The personal information consists of location, browsing, and behavioral information. To quote the report: *Even though several of the ISPs promise not to sell consumers personal data, they allow it to be used, transferred, and monetized by others and hide disclosures about such practices in fine print of their privacy policies.* The report further notes that because the ISPs control the traffic from your home and across the internet, they have access to vast data sets about you not accessible to businesses.

  Tom's Takeaway: In the U.S., privacy laws and regulations cover only specific scenarios and are limited by the adopting legislative group. As it stands now, the laws are fragmented and hard to navigate as each state tries to tackle the privacy issue on its own, ultimately possibly harming the very individuals the laws were intended to protect.

- **In an effort to hire cybersecurity professionals to attack company networks under the guise of a legitimate penetration test, the notorious cyber criminal group, FIN7, was identified as having established a seemingly legitimate cybersecurity company called "Bastion Secure."** By recruiting legitimate professionals, the group would ultimately have to pay them significantly less than individuals who knowingly will be committing illegal cyber crimes.

- **Microsoft reported that the hacking group responsible for the Solarwinds hack, Nobelium, has been actively targeting the global IT supply chain.** Approximately 140 resellers and IT service providers have been identified as being targeted, 14 of which are believed to have been breached. Microsoft has been notifying and working with those impacted.

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, the Firm has 14 offices in New York, New Jersey, Connecticut, Maryland, Florida, and Rhode Island and more than 1,000 professionals providing a complete range of accounting, auditing, tax, and management advisory services. PKF O'Connor Davies is led by over 100 partners who are closely involved in the day-to-day management of engagements, ensuring a high degree of client service and cost effectiveness.

The Firm is a top-ranked firm, according to Accounting Today's 2021 "Top 100 Firms" list and was recently recognized as one of "America's Best Tax Firms" by Forbes. PKF O'Connor Davies was named one of Vault's 2021 Accounting 50, a ranking of the 50 best accounting employers to work for in North America and ranked among the top 50 most prestigious accounting firms in America in a complementary Vault survey.

PKF O'Connor Davies is the lead North American representative of the international association of PKF member firms. PKF International is a network of legally independent member firms providing accounting, tax, and business advisory services in over 400 locations in 150 countries around the world. With its tradition, experience, and focus on the future, PKF O'Connor Davies is ready to help clients meet today's ever-changing economic conditions and manage the growing complexities of the regulatory environment