Cyber Roundup – October 2020

By Thomas J. DeMayo, Principal, Cyber Risk Management

Our readers know that every industry is impacted by cybercrime. They also know that individuals, as well, are targeted. When these attacks seriously affect the well-being of our school kids and hospital patients – as you will read in this edition – we are all outraged. If this outrage can be directed toward ensuring that your own business and personal computer technology is safeguarded, get an independent cyber assessment and find out what actions need to be taken. When you are ready, we are here for you.

Key Cyber Events

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

- **In the healthcare arena, the following cyber incidents occurred:**
    - The first death directly linked to ransomware happened in September. Dusseldorf University Hospital in Germany suffered a ransomware attack that impacted 30 of their internal servers. A patient, in critical condition on her way to the hospital, needed to be rerouted to an alternative hospital approximately 20 miles away as a result of the system's disruption. She expired enroute.
    - Universal Health Systems (UHS), one of the largest U.S. health systems, suffered a ransomware attack that impacted hospitals throughout the U.S. UHS claims that the electronic health record (EHR) systems were taken down to control the incident. Hospitals reverted to backup procedures and offline documentation methods.

Tom's Takeaway: We frequently think of ransomware and cybersecurity in terms of dollars lost; rarely do we equate it to human life. While this is the first directly linked death, the reality is this is more than likely to be one of many. The hope is that this incident serves as a wake-up call for not only every healthcare entity, but every business that is dependent on technology. Cyber criminals do not discriminate. You are a target.

- **The following school districts were impacted by cyber incidents:**
    - The Hartford, Connecticut public school system suffered a ransomware attack that contributed to the delay of the start of their school year.
    - Somerset Hills School District, New Jersey suffered a ransomware attack, disrupting the internal network and forcing the school to suspend in-person learning. Virtual learning was not impacted.
    - Haywood County School District, North Carolina suffered a ransomware attack. The attack, just like the other districts, resulted in not only system disruption, but the release of district information stolen as part of the attack.

- Clark County School District, Nevada suffered a ransomware attack during the first week of school. The District refused to pay the ransom, which resulted in the attackers releasing student information it had already stolen from the District.

- Fairfax County School District, Connecticut suffered a ransomware attack. The attack is still under investigation. As with Clark County, the attackers have released District information as part of the attack.

Tom's Takeaway: One recurring theme in the set of targeted industries is that school districts are a prime target. Further, what is at stake is not only the students' ability to learn, but also the private information of their parents. If you are connected to a school district, you must take action before an incident occurs. While you may not be able to completely prevent an attack, through prudent measures, you can limit the impact should it occur. Find out from your child's school or district the security measures they have taken. Key questions to ask: have they performed an independent cybersecurity assessment and what actions have they taken as a result.

- **The department of Veterans Affairs (VA) reported a breach that impacted 46,000 veterans and 13 community care providers supplementing the medical services provided.** While the details of the breach are still under investigation, it is believed that through a social engineering campaign, the attackers were able to gain access to an application managed by the VA Financial Services Center (FSC). The attackers changed payment details, diverting payments from the VA to the community care providers. In addition, the attackers may have gained access to sensitive personal veteran information such as the SSN. The VA is notifying impacted individuals on steps to take and will be offering one year of free credit monitoring.

- **An online database containing the personal details of hundreds of thousands of users across more than 79 dating websites was identified as being exposed on the internet.** The source of the breach is a third party company, Mailfire, that offers marketing tools. Not only was the personal identity information of the subscribers compromised, but also messages between users. The database has since been restricted.

- **Arthur J. Gallagher, a global insurance brokerage firm, reported a ransomware attack**. Details on the attack have not yet been released.

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.

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.