Cyber Roundup – July 2019

By Thomas J. DeMayo, Principal, Cyber Risk Management

While hope springs eternal, it's probably safe to say that we will never be 100% inoculated against cybercrime. That's why being on high alert continues to be the way to go.

That's also why we at PKF O'Connor Davies stand by to provide cyber assistance. Don't ignore the risk; we can help you face it.

Key Cyber Events

The following is a rundown of what happened during the month of June 2019. We welcome your comments, insights and questions.

- **The New York State Assembly passed the SHIELD Act (Stop Hacks and Improve Electronic Data Security Act).** The Act, if signed into law by the governor, will expand upon the existing breach notification requirements and require reasonable administrative, technical and physical security practices on any person or business collecting personal information on New York residents. Safeguards will include such things as employee cyber training and regular testing and monitoring of the company's information security controls and systems.

  Tom's Takeaway: This is a positive step forward in establishing expectations and accountability for any business that processes personal information. Should this bill be signed into law, we will release a special white paper on the specifics of this law and how to comply. Stay tuned.

- **Two Florida cities, Riviera Beach and Lake City, both suffered Ransomware attacks that resulted in the payment of the ransom to regain control of their systems and data.** Collectively, almost $1.1 million was paid out to the cyber criminals, with Rivera Beach paying $600,000 and Lake City $460,000. Both events were the result of a malicious e-mail received by an employee.

- **Baltimore, still in the process of recovering from the Ransomware attack last month, approved the use of $10 million in excess revenue to fund the additional costs of the ongoing recovery efforts.** In addition, the Governor of Maryland signed an executive order to strengthen the state's cybersecurity program. The order will formally establish the Maryland Cyber Defense Initiative and the creation of State Chief Information Security Officer.

  Tom's Takeaway: While Maryland is moving in the right direction, it is unfortunate that a major incident had to occur to push the movement. Cyber incidents can and will occur. The question is, are you ready? If you need assistance in understanding your cyber risk and how to effectively and practically manage and reduce that risk, we are always happy to help.

- **IT Managed Service Providers (MSPs) were again targeted to distribute Ransomware to their customers' systems.** Three managed service providers were identified as being breached with the cyber criminals leveraging the remote management tools of the MSP to infect the customer systems. MSPs were also targeted back in February of this year in an effort to distribute malware.

- **China has been linked to the hacking of at least 10 major cellular carriers and eight cloud services providers.** In both campaigns, it is believed that the motivation for the attacks is corporate espionage. The attack against the cellular carriers, dubbed Operation Softcell, believed to be in operation since 2017, targeted data related to specific individuals such as device details, physical location, source, destination and call duration. The attack against the cloud services providers, dubbed "Cloud Hopper," targeted major companies such as Hewlett Packard, IBM, Fujitsu, DXC Technologies, Dimension Data, NTT Data, Tata Consultancy Services, and Computer Sciences Corporation. The goal of the campaign was not to only obtain access to sensitive data and intellectual property of the providers, but also their customers.

- **Quest Diagnostics, Labcorp and Bioreference all reported breaches collectively impacting approximately 20 million individuals.** The incident was ultimately the result of a breach at a third party collection agency used by the companies, American Medical Collection Agency (AMCA). AMCA is believed to have been breached between August 1, 2018 and March 30, 2019. The information impacted contained Social Security Numbers, financial data, and medical information. Information specific to lab results was not compromised. Shortly after the breach AMCA's parent company, Retrieval-Masters Creditors Bureau, filed bankruptcy as a result of losing the business of the affected companies and other major customers and the significant costs incurred (approximately $4 million) responding to the breach.

- **The United States Custom and Border Protection (CBP) reported a breach that resulted in the exposure of photos of people's faces and license plates entering and leaving the country.** The incident was the result of a breached subcontractor that violated CBP security protocols and transferred the images to their own systems without authorization. The images impacted were collected over a month and a half period and impacted fewer than 100,000 people.

  Tom's Takeaway: Third-party risk is something every business needs to understand and manage. Any company, inclusive of an IT MSP, that will have access to your environment and/or store, process and transmit data on your behalf, needs to be assessed relative to the risk they present. Factors, such as the method of connectivity, the level of access to be provided, and the data they will handle, are all key considerations in determining the risk level. If you need assistance in developing a third-party risk management program or directly performing due diligence on a third party on your behalf, please feel free to contact me directly.

- **The United States launched a cyberattack against Iran in response to a downed surveillance drone by the country.** The offensive retaliatory cyberattack disabled Iranian systems that control rocket and missile launches.

- **North America's largest credit union, Desjardins Group, reported a breach impacting 2.9 million members.** The breach was the result of an employee. The employee used not only their own credentials, but tricked others in the credit union to provide theirs as well in order to bypass controls implemented by the credit union. The details exposed included such items as name, date of birth, Social Security Numbers, contact information and banking history. The employee has since been arrested.

  Tom's Takeaway: Nowadays, we often equate information and cybersecurity breaches with external parties. The reality is that insiders also pose a significant threat that cannot be overlooked or underestimated. A motivated insider is at an incredible advantage compared to an external party, having a powerful tool in their arsenal – trust. When designing your information and cybersecurity program, you must account for the insider threat across the three main pillars of control: people, process, and technology.

- **NASA reported a breach as a result of an unauthorized device plugged into their network.** The cyber criminals, who remained undetected for almost a year, exfiltrated data related to the Mars missions. While details of the incident are still being investigated, it is believed the attack was carried out by an advanced cybercriminal group.

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, eleven offices in New York, New Jersey, Connecticut, Maryland and Rhode Island, and more than 700 professionals, the Firm provides a complete range of accounting, auditing, tax and management advisory services. PKF O'Connor Davies is ranked 29th on *Accounting Today*'s 2019 "Top 100 Firms" list and is recognized as one of the "Top 10 Fastest-Growing Firms." PKF O'Connor Davies is also recognized as a "Leader in Audit and Accounting" and is ranked among the "Top Firms in the Mid-Atlantic," by *Accounting Today.* In 2019, PKF O'Connor Davies was named one of the 50 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.