PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Cyber Roundup – June 2023

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

Cybersecurity is not an expense; it is a necessary investment — an investment in the continued operations of your company and the trust of those who may rely on you. As you will see later in this publication, financial penalties were exacted in May for cybersecurity failures. The Regulators are no longer sympathetic to leaving a cyber threat unresolved. Our Firm can help educate and protect those needing cyber assistance. As with any service, there is a cost; however, with a proactive strategy is often less than the cost of avoiding the legal, financial and reputational damage is essential to your business. As we say: ***if you need us, we are here.***

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.

- **The National Security Agency (NSA) released an updated set of best practices in securing your home network**. The article can be found here. Like many other things, cybersecurity starts at home; I encourage you to read the article.

- **Financial penalties for failures in cybersecurity programs was a common theme in May.** Here are some of them:

  - **The Department of Health and Human Services issued a $350,000 fine to MedEvolve, a practice management software and services provider.** The fine was the result of a File Transfer server containing medical information that was incorrectly secured and accessible to the public internet.

  - **The New York Department of Financial Services (NY DFS) issued a $4.25 million fine to OneMain Financial as a result of multiple material failures identified in their cybersecurity program.** Failures ranged from vendor management, access control, security awareness training and vulnerability management. Of greatest concern: many of these issues were identified and made aware to the Company, but no action was taken to remediate. The Superintendent of the NY DFS made it clear that the agency is committed to the cybersecurity regulation passed in 2017 requiring regulated entities to have sufficient cybersecurity programs to protect New York residents' personal information.

  - **The New York State Attorney General fined Practicefirst Medical Management Solutions $550,000 for failure to patch a known vulnerability in their firewall.** This resulted in the breach of 1.2 million personal records. In addition, Practicefirst did not perform activities such as penetration testing, vulnerability scans, or other proactive measures that would have facilitated the detection of the issues.

  - **Kronos Inc., a human resources management solutions company, agreed to a $6 million settlement as a result of a ransomware event.** The incident occurred in 2021 and was the result of insufficient cybersecurity practices.

- **The Department of Justice announced the take down of a highly sophisticated Russian-developed malware that has been unknowingly operating for almost two decades.** The

malware, dubbed “Snake,” has been used over that time to actively steal secrets from at least 50 NATO members, inclusive of the United States.

- **Montana becomes the first U.S. state to ban TikTok.** The law, which will go into effect January 1, 2024, would prohibit the operation of the app on any device in Montana. To date, TikTok has only been banned on government-owned devices. Potential fines of $10,000 per day could be levied for any violators of the law, inclusive of app stores such as Apple and Google. The Governor declared the goal is to protect Montanans’ personal data from the Chinese government.

- **In a significant ruling, a New Jersey appellate court declared that insurers cannot use an act of war argument to deny cybersecurity claims against non-military businesses.** The ruling was related to a claim made by pharma company Merck that suffered significant damage from the Russian-backed global ransomware event “NotPetya” which occurred in 2017. The claim was denied as the insurers declared the losses tied to an act of war.

- **U.S.-based dental benefits manager, MCNA Insurance Company, suffered a breach of their systems by a cyber actor.** The breach resulted in the exposure and exfiltration of approximately 9 million highly sensitive personal records, inclusive of such information as social security numbers, driver licenses, government IDs, insurance information and dental records. Information such as this is highly prized by cyber criminals as it can be used and sold to facilitate identity theft. The Company has notified the impacted individuals.

- **Ransomware events continued to be prolific in May**. The following are some of the key events:

  - **The City of Dallas, Texas suffered a major ransomware attack on May 3 impacting major city services**. As of June 5, 10% of the services continued to remain offline.

  - **The San Bernardino County, CA Sheriff’s Department suffered a major ransomware attack resulting in the payment of a $1.1 million ransom.** While insurance covered almost half, the County had to pay the $500,000+ balance.

  - **Bluefield University, West Virginia, suffered a ransomware attack.** It resulted not only in the encryption of their systems and the exfiltration of their data, but the cyber criminals also gained access to the University’s emergency alert system and actually used it to send text messages and emails to students and faculty warning them they would circulate their information to the public if the University did not pay.

  - **North Carolina’s Raleigh Housing Authority suffered a ransomware attack shutting down key systems.** The agency is working with state and federal agencies to help resolve the issue. The full extent of data that may have been impacted is not yet known.

  - **The U.S. Marshals computer network remained down in early May — ten weeks after being subject to a ransomware attack.** The attack impacted a critical system used to track suspected criminals through mobile phones, email and the internet. The U.S. Marshals declared that once restored, improved cybersecurity measures will have been implemented to prevent recurrence.

  - **The 90’s rock band, Smashing Pumpkins, paid a ransom to prevent a hacker from leaking the band’s songs that were slated for release in May.** The payment was made as the perceived risk of the songs leaking could have had a significant impact on promotion and sales.

  - **Dole Food Co. stated in their first quarter earnings report that they incurred $10.5 million in direct costs because of a ransomware event in February.** It impacted many of their servers and workstations and disrupted operations.

  - **Richmond University Medical Center (RUMC), based in Staten Island, NY, suffered a ransomware attack on May 6.** It disrupted internal systems and resulted in the failover of manual methods of care and monitoring.

Tom's Takeaway: As a lifelong resident of Staten Island, this ransomware attack on RUMC hits close to home. In addition to my family having medical procedures at the hospital, all three of our daughters were born there. It is easy to read or write about cyberattacks and not be entirely sympathetic to the human impact unless it involves a target we know. The reality is that these cyberattacks can be devastating – financially, reputationally and emotionally. These attacks will continue until all of us, personally and professionally, take measures available to protect ourselves and each other.

Contact Us

Thomas J. DeMayo, CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
Partner
Cybersecurity and Privacy Advisory
tdemayo@pkfod.com | 646.449.6353

Nick DeLena, CISSP, CISA, CRISC, CDPSE
Partner
Cybersecurity and Privacy Advisory
ndelena@pkfod.com | 781.937.5191