PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Cyber Roundup – January 2023

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

None of us is safe as individuals or businesses from a cyberattack; however, taking steps before it actually happens can prevent its eventuality. Our cyber team can review your existing safeguards and work with you to harden them. We can suggest other methods as well and engage with your staff to try and insulate their work product. Nothing is 100%, but the closer we come to that the better our chance to avert a successful strike.

Contact me at tdemayo@pkfod.com and we can set up a teleconference or televisit.

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 Hive ransomware group successfully breached Knox College, Galesburg, Illinois, taking systems offline and gaining access to highly sensitive information such as social security numbers and medical records.** The ransomware group took an additional measure of reaching out to the impacted faculty, staff and students directly to let them know they had their data.

- **Hope College in Holland, Michigan is being subject to a pair of class action lawsuits as a result of a ransomware attack that was suffered in the fall.** The lawsuit accuses the school of negligence, breach of fiduciary duty and violating the Michigan Consumer Protection Act. The beach impacted approximately 150,000 individuals.

  Tom's Takeaway: The prior two bullet points make it clear that the education sector is a key target for cyber criminals. The reputational, operational and financial implications can be significant. Establishing a meaningful and effective cybersecurity program is essential to providing a safe and nurturing educational environment. If you need assistance in evaluating or establishing your cybersecurity program, we can help.

- **Long Island's Suffolk County which suffered a devastating ransomware attack in the fall disclosed that the forensic analysis of the attack revealed that the attackers first gained access to the network in December of 2021.** The attackers gained a foothold into the network by leveraging a known vulnerability that went unpatched. The attackers successfully managed to gain larger access to the network in the summer and ultimately launched their attack in the fall.

  Tom's Takeaway: We have emphasized the importance of patching and overall vulnerability management in many issues of *Cyber Roundup* over the years. This again serves as a reminder that a strong process to identify, prioritize and resolve vulnerabilities is critical.

- **Security researchers discovered a vulnerability in Sirius XM's connected vehicle systems that would allow them to start, unlock, honk the horn and locate the vehicle with only knowing the VIN.** The system is used in more than 10 million systems across North America. The flaw has since been fixed.

- **Brooklyn Hospital Group, One Brooklyn Health, that consists of three facilities, suffered a ransomware attack that resulted in operations falling back to traditional paper practices.** The attack had taken offline key clinical applications. The attack did not impact patients and the

facilities remained open to provide care. The attack impacted operations for over a month as the facilities tried to restore their systems.

- **The Metropolitan Opera suffered a cyberattack that disrupted their website, box office, call center and payroll system.** While shows continued, the Opera had to resort to selling all seats for $50 each, significantly impacting revenue. Manually created tickets were handed out with seat numbers written on the back in black marker. To cover the payroll system being down, checks were manually cut to cover 3000+ workforce. The systems were down for approximately 9 days before they could be fully restored.

Contact Us

Thomas J. DeMayo, CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
Principal
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