PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Cyber Roundup – March 2023

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

As you will read below in one of the monthly incidents, businesses continue to be held accountable for their failures to protect against electronic intrusive breaches to their data. This will continue to be an increasing trend. As we often say, cybersecurity is not a business expense, it's really a business necessity. For any company that handles sensitive data, not having a qualified Chief Information Security Officer (CISO) to help drive their cybersecurity strategy could prove to be costly. While full-time CISOs may be cost prohibitive, a fractional CISO – known as a virtual CISO or vCISO – can be a valuable and cost-effective solution. We serve as vCISO for many organizations ranging from not-for-profits to highly regulated entities. Should you be interested in exploring a vCISO option, we would be happy to assist.

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.

- **January 24, 2023 marked the one-year anniversary of the Russian invasion of Ukraine.** The Cybersecurity and Infrastructure Security Agency (CISA) issued an advisory on February 23, 2023 alerting that U.S. and European nations may experience disruptive and defacement attacks against their websites. The advisory, found here, reminds organizations to remain vigilant in light of the continued threat and contains pertinent information on how to protect your organization.

- **DNA Diagnostic Center has agreed to pay $400,000 in a settlement with the Attorney Generals of Pennsylvania and Ohio for a data breach that occurred in 2021 impacting 2.1 million individuals.** The breach included highly sensitive information, such as Social Security numbers and payment card information. The settlement agreement states that the Company made deceptive statements in their privacy policy regarding the protection of personal information and failed to employ reasonable practices to protect against and detect cyber intrusions. In addition to the fine, it agreed to hire a Chief Information Security Officer (CISO), conduct regular risk assessments and develop an incident response plan.

- **GoDaddy, a major web hosting and domain registrar, reported in their securities filing that they suffered a breach that lasted approximately three years.** The breach resulted in the theft of source code, customer and employee login information and redirected customers' websites to malicious sites. GoDaddy is working with law enforcement and forensic experts to identify the root cause of the issue.

- **The European Union Commission issued a ban on the installation and usage of TikTok on Commission-owned devices and employee personal devices enrolled with their mobile device management.**

  Tom's Takeaway: The EU Commission's extension of the block of TikTok to employees' personal devices touches on an area many businesses feel they do not have the right to enforce. I am often asked how can the business tell the employee what they can do on their own phone? My response is that the business has a right as long as they disclose that right in their policy and the employee chooses to accept the terms of that policy. Should the employee not agree to the terms, the connection of the device is not allowed. What the business has to decide if the use of the phone is necessary for the performance of their job function or not. If necessary, they have to provide the employee a business-controlled phone as the employee does have the right to refuse the use of their personal device. If the employee is not required, then they simply cannot connect. What the

business needs to appreciate is that the device, personally owned or not, becomes a connection point to business data and ultimately a risk that needs to be managed.

The following are key ransomware-related events that occurred in February.

- **To ensure no out-of-pocket costs for their victims, operators of the ransomware variant Hardbit has begun requesting insurance details of their victims.** The goal is to negotiate a payment amount that will be fully covered by the insurance.

- **Tallahassee Memorial HealthCare, located in Florida, suffered a ransomware attack resulting in the cancellation of non-emergency procedures**. The Hospital shut down all IT systems to proactively address the threat. Emergency cases were rerouted to other hospitals.

- **In a report issued by Trend Micro, they claim that for every ransomware victim that pays the ransom, 6-10 new attacks are funded.**

- **The City of Oakland suffered a ransomware attack that resulted in a number of non-emergency City systems going offline.** The City has not paid the ransom demand which has resulted in the attackers beginning to release the information stolen from the City computers online. The data posted to date contains employee IDs, passports, Social Security numbers and other documents. Only a subset has been released to date with a threat to release it all if payment is not made. The City is working with law enforcement and forensic experts to further investigate the attack.

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