PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Cyber Roundup – January 2021

By Thomas J. DeMayo, Principal, Cyber Risk Management

Shakespeare's King Lear said "*You will gain nothing if you invest nothing.*" Although used in a different context, this excerpt might apply to those businesses that don't invest (time and money) in safeguarding their IT infrastructure. As you know and will read further about in this issue of *Cyber Roundup*, your data is subject to swatting, spoofing, phishing, exfiltrating, etc. at the will of hackers and ransom seekers. Although there are no guarantees, cut your business risk of such events by engaging us to help you secure your data and platforms. We are at your service.

Key Cyber Events

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

- **According to a joint study by security vendor McAfee and the Center for Strategic and International Studies, cybercrime cost the world economy $1 trillion in 2019.** That is approximately a 50% increase from the $600 billion estimate in 2018.

- **The FBI issued an alert that cyber criminals are leveraging breached home security systems to "swat" their victims.** Swatting is a tactic in which the criminal will call emergency services with fake emergencies. The hacked security systems allow the criminals to watch the event unfold as the law enforcement respond to the residence. In the past hackers would spoof the phone number when contacting the authorities; however, the tactic has now evolved to contact the services directly from the security device, further making the call seem authentic. The security devices are being compromised as a result of the cyber criminals leveraging known breached credentials of their victims.

  Tom's Takeaway: Any internet-connected device that is password protected will be subject to compromise. The only way to prevent this type of incident is to use multi-factor authentication, if available, or use a strong unique password for these devices. Passwords are certainly hard to remember; however, tools such as a password manager exist to help you balance having greater security without the need of remembering a multitude of different passwords.

- **GoDaddy made the headlines in December for sending a phishing e-mail to their employees promising a Christmas bonus.** The email offered a $650 bonus and required a form to be completed. A phishing e-mail is a fake e-mail sent by a company with the intention of seeing those who click or provide information in order to serve as more targeted awareness training. Approximately 500 employees failed the test. The test was perceived to be insensitive.

  Tom's Takeaway: Phish testing your employees is one of the best things you as a business can do to help train your employees. While I don't know the full details of GoDaddy's program, a successful and embraced awareness program starts with clearly communicating to your employees that you plan to do such testing and why. The end result is not only to help protect the company, but protect the employee as well. As a Firm, we phish test our employees a minimum of three times per month, and, yes, we include holiday type offerings such as a free turkey from our managing partner during the Thanksgiving holiday. The goal is not to victimize, entrap, or hurt feelings, but to ensure as a business we are addressing one of our biggest risks. No technology will prevent phishing, making it critical we know how well we are training and empowering our employees to help protect the Firm, its clients, and themselves. Phishing is without question a key risk to every business. The more you can phish and train, the better. If you need assistance in designing an effective training program, please contact us.

- **Fake Facebook ads were leveraged by cybercriminals to trick the users of the platform to provide their Facebook username and password.** The cyber criminals would purchase Facebook ads representing a legitimate company offering a product or service. Should the user click the ad, they were presented with a fake Facebook login page designed to capture and steal their credentials. In total, over 615,000 users fell for the scam.

- **A six-month study by security researchers resulted in the identification of approximately 43 million medical images and personal information stored in 2,140 servers across the globe that have been incorrectly secured.** The images were freely available for anyone to access. The images were often accompanied with the necessary information to identify the individual. The images were associated with a multitude of different companies and providers.

  Tom's Takeaway: In a cyber landscape dominated by active cyberattacks, it's easy to forget that a lot of data breaches are still the result of incorrectly-configured systems. An incorrectly-configured system is an entirely-preventable event with the appropriate procedures in place to ensure data protection. Systems are often deployed in haste and at times by individuals with insufficient skill sets. A well-designed security program will include a culture of ensuring security by design and by default prior to any system being exposed.

- **Cellular provider, T-Mobile, alerted to its fourth data breach in three years.** The incident is believed to have impacted 200,000 customer accounts. While no sensitive information was breached, unauthorized access to customer accounts exposed information such as customer numbers, subscribed lines, and call details.

- **In a report by security vendor, CrowdStrike, 51% of all incidents they investigated in 2020 was associated with ransomware.** The report further notes that ransomware gangs have become increasingly sophisticated, allowing them to stay in the breached victim's networks longer and cause greater damage. Ransomware has become a common theme of our *Cyber Roundup*. The following is a summary of Ransomware events in December:

  - In an effort to harass and secure payment from their victims, ransomware gangs have been increasingly calling their victims over the phone. The calls appear to be coming from an outsourced call center operation. Below is a sample transcript obtained from zdnet.com.

    "We are aware of a 3rd party IT company working on your network. We continue to monitor and know that you are installing SentinelOne antivirus on all your computers. But you should know that it will not help. If you want to stop wasting your time and recover your data this week, we recommend that you discuss this situation with us in the chat or the problems with your network will never end."

  - Huntsville City School District in Alabama suffered a ransomware attack. The district alerted impacted staff and students that potentially sensitive information had been compromised as a result of the attack. The District did not pay the ransom and is offering credit monitoring services for those who may have been impacted.

  - Baltimore County School System reported a ransomware breach that resulted in 115,000 students unable to connect to their virtual classrooms.

  - Whirlpool, the American-based manufacturer, suffered a ransomware attack. Whirlpool was able to restore operations; however, the ransomware gang also extracted data from Whirlpool systems prior to the system encryption event. Sample listings of potentially sensitive data extracted have been posted to the ransomware gang's blog on the dark web.

  - A prominent cosmetic surgery group, The Hospital Group, suffered a ransomware attack. As with the other companies noted, not only were systems encrypted, but data exfiltrated as well. The ransomware gang has claimed to have extracted 600GB of sensitive data and is threatening to post the data unless the ransom is paid.

Contact Us

The pandemic has thrust upon the world many changes for better or for worse. As a business, this is a time to really step back, evaluate your current technical and data landscape, and make sure you are positioned to come out of this better, stronger, and more efficient. The good news is you don't have to do it alone. At PKF O'Connor Davies, we have the resources to help you navigate your path forward across all facets of your business. We encourage you to contact us **today** as you continue down that path of success.

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, fourteen offices in New York, New Jersey, Florida, 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.