PKF
O'CONNOR
DAVIES
ACCOUNTANTS AND ADVISORS

Cyber Roundup – November 2020

By Thomas J. DeMayo, Principal, Cyber Risk Management

The speed with which cybercrime continues to adapt to new technologies, preventative and resistance measures is matched by the creativity with which today's criminals create new opportunities to wreak havoc. As predicted, cybercrime is on the rise. Losses and damage are expanding. Healthcare systems are being compromised with lethal implications. Even the sanctity of home is at risk when our vulnerable cameras are hacked Cyber thieves are emboldened enough to risk exposure by donating illegally gotten proceeds to charities in need – and feel pride of purpose! Fortunately, cybersecurity experts are keeping pace, performing assessments and implementing strategic protection tactics to help safeguard businesses, employees and individuals from punishing financial and reputational consequences. Staying informed is the first key step, which is why we provide the vital updates below. Please contact us for support services.

Key Cyber Events

The following is a rundown of the schemes, hacks and breaches that have unfolded in recent months. We welcome your comments, insights and questions.

- 36 billion records have been breached across 2,953 reported incidents as of the end of Q3 2020. This represents an increase of 8.3 billion records since the end of Q2 and further solidifies 2020 as a new record-breaking year for data breaches. Furthermore, 21% of the breaches reported were the result of ransomware as cyber criminals made a push not only to encrypt, but to release, their victims' data.

- The FBI issued a ransomware warning that cyber criminals are actively and aggressively targeting the U.S. healthcare system. According to Checkpoint Security, ransomware attacks against hospitals and providers surged 71% compared to the prior month. Currently five healthcare systems have been impacted.

  Tom's Takeaway – It was only a few months ago that we wrote about the first death directly related to a ransomware event. Everyone is a target. That is a fact that no business or individual can ignore -- especially healthcare providers, as the operations of their IT systems can mean the difference between life or death. From a business perspective, I fully understand that a company would not want to spend money on cybersecurity; however, cybersecurity can no longer be viewed as an expense, but rather, a necessary investment in the success of your operations. A recent study by BitSight and Solactive demonstrated that a company's cybersecurity effectiveness can serve as an indicator of its overall performance, noting that companies with mature cybersecurity programs outperformed their competitors.

- According to a study by Arctic Wolf, the number of company credentials (usernames and passwords) exposed on the dark web has increased 429% this year. Attackers actively use these breached credentials in "password stuffing" or "credential stuffing" attacks, in which cyber criminals use the breached password in an attempt to gain access to the hacked person's other accounts – betting that many people use the same password for numerous accounts, which is often the case. The following businesses were directly targeted by a credential stuffing attack in October:

  - Robinhood, an online trading platform, experienced a breach of nearly 2,000 accounts as a result of credential stuffing.
  - Sam's Club actively alerted customers that their accounts may have been accessed by unauthorized individuals as a result of credential stuffing.

  - Capcom, an electronic gaming company, suffered a data breach as a result of credential stuffing that lead to a breach of internal systems and files.

  Tom's Takeaway – Credential stuffing is a real threat for which businesses need to prepare. The three best methods to combat credential stuffing are multi-factor authentication, dark web monitoring and employee awareness training. Dark web monitoring, in which a business proactively monitors the dark web for stolen credentials, facilitates alerting the hacked employee to change any necessary credentials. Dark web monitoring is a very affordable solution. If you are interested in learning about our Dark Web Monitoring solution, please feel free to contact us. As a courtesy, we will run a complimentary dark web scan on your business to assess your current exposure.

- A cybercriminal group has posted for sale three terabytes of recorded home videos from compromised internet cameras. The group will offer a sample of approximately 4,000 videos to interested parties. The entire collection can be downloaded for a fee or, for a subscription fee of $150, allows lifetime access. The videos were specific to home-based cameras to capture the activities inside people's homes.

  Tom's Takeaway – When I perform cybersecurity awareness training for clients, I always emphasize one key point: *with connectivity comes risk*. The instant you connect to the internet, you have the potential of becoming a victim. While I certainly understand the need for security cameras, don't assume that your camera is inherently secure. Remember, if you can get to it remotely, someone else can too, so you should implement the proper controls to restrict access. Of greater concern is whether the device you are connecting is even capable of being secured.

- Business E-Mail Compromise (BEC) is now responsible for $26 billion in global losses and accounts for 40% of cybercrime losses. The average current payout is $80,000. 25% of BEC attacks originate from within the United States, specifically Texas, New York, California and Florida. Furthermore, Money Mules, people who, knowingly or unknowingly, enable these scams by facilitating the illegal movement of money, are critical to successful BEC operations. These players are also located predominately in the United States. The full report is located here.

  - The Town of Franklin, in Boston, suffered a BEC as a result of a phishing - that resulted in the transfer of $522,000.
  - The Republication Party of Wisconsin reported that $2.3 million was lost as a result of BEC fraud in which invoices were altered to direct payments to fraudulent accounts belonging to the criminals.
  - Three Swiss universities suffered a combined six-figure total loss as a result of a BEC scam that enabled unauthorized access to the institution's payroll system and, ultimately, the changing of employee payment instructions.
    Between June and September 2020, the education sector fell prey to twice as many BEC scams as it had in the past. Google Gmail accounts, the primary e-mail system used by most education institutions, was the main mechanism used by cyber criminals to facilitate their attacks.

  Tom's Takeaway – Business e-mail compromise can trace its roots back to the original Nigerian Prince scams that started circulating in the 1980s in the form of traditional snail mail. BEC was quickly adapted to the electronic realm in the early days of the internet. The scam has certainly evolved and has become more sophisticated over time, but the premise of the tactic remains the same: manipulation of an individual to perform an action. This type of fraud is very preventable with the appropriate policies, training and technical controls. As part of either our cyber assessments or fraud assessments, this is one of the key areas in which we help clients avoid becoming victims.

- In the spirit of "honor among thieves," the cyber criminal group Darkside has made charitable contributions to two organizations using funds they stole from victim organizations. In its online blog post, the group emphasizes that it only targets large and profitable organizations for its cyber theft. Its representatives are quoted in the post as saying, "We think that it's fair that some of the money the companies have paid will go to charity. No matter how bad you think our work is, we are pleased to know that we helped changed someone's life." One of the beneficiaries, Children International, has already stated they will not be accepting the funds.

- The notorious REvil ransomware group has offered $1 million in an effort to attract new recruits to spread its ransomware. REvil falls under the category of "Ransomware As A Service." In this model, REvil is responsible for the development of the actual code and product that will carry out the ransomware; however, the affiliates are responsible for the distribution. In exchange for the ransomware product, the affiliates pay REvil 20-30 % of their proceeds from the ransoms they collect. As our world evolves into an increasingly complicated technology-driven arena, cybersecurity experience is more and more essential. Our specialists are ready to answer questions and share their knowledge to help you protect yourself, your clients and the integrity of your business information.

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, twelve offices in New York, New Jersey, 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.